Sözde Diferansiyel Faktörler Ve Blok Şifre Atakları Zaman Karmaşıklıkları

Program Kodu: 1001

Proje No: 115E447

Proje Yürütücüsü:
Doç. Dr. Ali DOĞANAKSOY

Bursiyer:
Merve ÖĞÜNÇ

MART 2017
(Revizyon Mayıs 2017)
ANKARA

1. Önsöz

Şifreleme algoritmalarının anahtar uzunlukları mevcut teknolojik durum göz önüne alınarak belirlenir ve dünyadaki bütün işlem gücüne sahip cihazlar paralel olarak çalıştırıldığında bile anahtarın elde edilememesi beklenir. Dolayısıyla günümüzde simetrik şifreleme algoritmaları güvenliği için en az 128 bitlik anahtarlar kullanılmaktadır. Bazı mevcut algoritmalar 80 bitlik anahtar kullanmakta ve bu algoritmalar bazı kriptograflar ve güvenlik uzmanları tarafından güvenli olarak düşünülmektedir. Ama TÜBİTAK tarafından desteklenen bu projenin sonuçlarından bir tanesi, özel donanım kullanmadan bile ekran kartlarının paralel işlem gücü kullanılarak 80 bitlik anahtarların ele geçirilmesinin istihbarat birimleri gibi yüksek işlem gücüne sahip birimler açısından mümkün olduğudur.

Algoritmaların uzun anahtarlar kullanması, teorik yollarla elde edilen kriptanaliz sonuçlarının da genellikle yüksek işlem gücüne ihtiyaç duymasına ve dolayısıyla pratikte doğruluklarının kontrol edilememesine neden olmaktadır. Bu projede ekran kartlarının yüksek paralel işlem gücü kriptografik algoritmalar için optimize edilerek sıradan işlemcilere kıyasla 6-20 kat daha fazla şifreleme işlemi yapmanın mümkün olduğu gösterilmiş, doğruluğu pratikte kontrol edilmemiş teorik sonuçlar kontrol edilmiş ve yeni zafiyetler taranmıştır.

Ayrıca projede yakın zamanda sunulan ve diferansiyel türü atakların zaman karmaşıklığının azaltılmasında kullanılan diferansiyel faktör kavramı incelenerek bu teori önce geliştirilmiş, daha sonra da sözde diferansiyel faktörler adıyla genişletilerek atak karmaşıklıklarının büyük miktarlarda azaltılabileceği gösterilmiştir.

2. İçindekiler

2.1 Tablo Listesi

2.2 Şekil Listesi

2.3 Revizyon Bilgisi

Bu sonuç raporu danışman/raportör görüşleri doğrultusunda yeniden hazırlanmıştır. Yapılan değişiklikler şu şekildedir:

1. Kapak sayfasındaki sayfa numarası kaldırılmıştır.
2. Ana metinden önceki sayfalar Romen rakamları (i, ii, …) ile numaralandırılmıştır.
3. Raporun tamamı gözden geçirilerek birçok yazım yanlışı ve devrik cümle düzeltilmiştir.

3. Özet

Blok şifrelerin büyük kısmının güvenliği karışıklık (confusion) katmanında yer alan değişim kutularının (S-box) kalitesine bağlıdır ve literatürdeki değişim kutuları özellikleri bu kutuları tek başlarına incelemektedir. Yakın zamanda Tezcan tarafından önerilen diferansiyel faktör kavramı ise değişim kutularını genellikle kendilerinden önce gelen anahtar ekleme katmanıyla birlikte incelemektedir. Diferansiyel faktörlerin varlığı, bu özelliği bilmeden teorik yollarla elde edilmiş literatürdeki atakların yanlış olmasına neden olmaktadır. Ve bu yanlış ataklar diferansiyel faktörler dikkate alınarak düzeltildiğinde elde edilen bu yeni atağın zaman karmaşıklığı değişmektedir. Bu proje öncesine kadar diferansiyel faktörler sadece SERPENT şifresine verilen ataklar için kullanılmıştır. Bu şifre için literatürdeki ataklar düzeltilmiş ve zaman karmaşıklıkları azaltılmıştır.

Bu çalışmada öncelikle diferansiyel faktörlere sahip yeni blok şifreler belirlenmiştir ve diferansiyel faktörlerle ilgili yeni teorik gözlemler elde edilmiştir. Daha sonra literatürdeki diferansiyel faktöre sahip algoritmalara yapılan diferansiyel atakların hepsi incelenmiş ve PRIDE, RECTANGLE, PRESENT ve LBLOCK şifrelerine literatürde verilen ataklar düzeltilmiştir. Bu düzeltilmiş atakların zaman karmaşıklıkları yeniden hesaplanmıştır. Diferansiyel faktörler daha sonra projenin asıl hedefi olan sözde diferansiyel faktörlere genişletilmiş ve SERPENT şifresine bilinen en iyi ataklar elde edilmiştir. Ayrıca ASCON şifresine ilk defa imkansız ve olası olmayan diferansiyel ataklar elde edilmiştir.

Ekran kartlarının paralel işlemlerdeki yüksek gücünün kriptografiye olan etkilerini göstermek için A5/1, AES, CRYPTO1, DES, 3DES, PRESENT, SERPENT şifreleri CUDA programlama dili kullanılarak optimize edilmiştir. Bu optimizasyonlar sonucunda

- AES şifresinin bilinen en hızlı kodu elde edilmiş (Intel işlemcilerin AES donanımsal desteğinden daha hızlı)
- CRYPTO1 şifresindeki zafiyetler kullanılarak ODTÜ'nün akıllı kart özellikli kimlik kartlarını birkaç saatte kopyalamanın mümkün olduğu gösterilmiş
- PRESENT gibi 80 bit ya da daha kısa anahtar kullanan algoritmaların kaba kuvvet saldırılarıyla pratikte kırılabileceği gösterilmiş
- SERPENT şifresine verilen teorik ataklar pratikte doğrulanmış ve gerçek zaman karmaşıklıkları elde edilmiş

- A5/1 şifresinin zayıflıkları ve kısa anahtarı nedeniyle ekran kartlarını aylarca kullanarak tablo oluşturacak kişilerin GSM görüşmelerini eş zamanlı kırarak dinleyebileceği gösterilmiştir

Anahtar Kelimeler: diferansiyel faktör, kriptanaliz, ekran kartı, zaman karmaşıklığı

4. Abstract

Security of block ciphers mainly depends on the confusion layer where generally S-boxes are used. Known security properties of S-boxes consider the S-boxes alone. However, a recent property called differential factor proposed by Tezcan considers the S-boxes together with the key addition layer. Attacks obtained by theoretical methods that do not consider differential factors might be wrong in practice. And correcting these attacks would result in a different attack and time complexity. Before this Project, differential factors were only applied to the differential-linear attacks on SERPENT.

In this work, new block ciphers with differential factors are detected and theory of differential factors is improved. Then, all of the differential variant attacks on these ciphers are analyzed and the attacks on PRIDE, RECTANGLE, PRESENT, and LBLOCK are corrected. Their time complexities are recalculated. Differential factors are extended to quasi-differential factors. Best attacks on SERPENT are obtained by using quasi-differential factors. Moreover, impossible and improbable differential attacks on ASCON are provided for the first time.

To show the effects of parallel processing power of GPUs on cryptography, we optimized A5/1, AES, CRYPTO1, DES, 3DES, PRESENT, SERPENT ciphers for GPUs using the CUDA programming language. With these optimization

- We obtained best known AES encryption speed (even faster than hardware instruction set of Intel processors)
- Using the weaknesses of the CRYPTO1 cipher, we showed that METU ID cards, which are smartcards, can be cloned in hours
- Ciphers like PRESENT with 80 or less key bits can be broken in practice by brute force attacks using only GPUs
- We practically verified the correctness of the theoretical attacks on SERPENT and reduced the time complexity of these attacks
- We showed that attackers can listen any GSM communication by genrating rainbow tables via GPUs in a short time using the weaknesses and the short key of A5/1

Keywords: differential factor, cryptanalysis, GPU, time complexity

5. Sonuç Raporu

5.1 Giriş

Blok şifreler iyi tasarlandığında güvenlikleri anahtar uzunluğuna dayanır. Örneğin k bitlik anahtar kullanan bir blok şifreyi kaba kuvvet yöntemiyle kırmak için 2^k adet şifreleme işlemi yapılır ve k sayısı en az 128 seçildiğinde günümüz bilgisayarlarının ya da işlem kapasitesi olan bütün cihazların hepsini kullandığımızda bile bu kadar işlemi yapmamız mümkün değildir. Eğer bir blok şifre iyi tasarlanmamışsa, diferansiyel veya lineer ataklar gibi istatistiksel ataklar sayesinde kaba kuvvet yönteminden daha az zaman karmaşıklığı ile şifreyi kırmak mümkün olabilir. Bu ataklar genellikle teorik yollarla elde edilmektedir ve kişi ya da küçük kurumlar bu atakların doğruluklarını kontrol etmek için gereken işlem gücüne sahip değildir.

Bu projede ekran kartlarının paralel işlem gücü kullanılarak sıradan işlemciler ile yapılması yıllar sürecek kriptografik işlemler günler mertebesine indirilmiş ve bu sayede önceden kontrol edilememiş teorik sonuçlar pratikte kontrol edilmiştir. Aynı zamanda ekran kartları için optimize ettiğimiz şifreler sayesinde 80 bitlik ya da daha kısa anahtar kullanan algoritmaların artık güvenli olmadığı gösterilmiş ve elde ettiğimiz AES şifreleme hızı CPU ve FPGA'lerin ötesine geçmiştir. Bu sonuçlar sayesinde ekran kartlarının kriptografik işlem hızlandırıcı olarak kullanılması sonucunda dosya ya da disk şifreleme kullanan kullanıcıların çok daha iyi performans elde edebileceği gösterilmiş, SSL sunucuları gibi çok fazla şifreleme işlemi yapan sunucuların ekran kartları kullanılarak rahatlatılabileceği gösterilmiştir. Ayrıca bu hızlanma ile parola tabanlı anahtar üretme yöntemi kullanan sistemlerde parola unutulduğu zaman parolanın kaba kuvvetle elde edilme süresi azaltılmıştır.

Projede ayrıca teorik atakların pratikte yanlış olmasına neden olan değişim kutusu özelliği diferansiyel faktörler incelenmiştir. Bu teori geliştirilmiş, literatürdeki ataklar düzeltilip gerçek zaman karmaşıklıkları hesaplanmış ve yeni ataklar bulunmuştur. Ayrıca diferansiyel faktörler sözde diferansiyel faktörlere genişletilerek mevcut teorik atakların pratikte çok daha hızlı çalışabileceği gösterilmiştir.

5.2 Literatür Özeti

Birçok blok şifre lineer olmayan yapı olarak sadece vektörel boole fonksiyonu olan değişim kutusu (S-box) kullanır. Diferansiyel kriptanaliz (Biham ve Shamir 1991) ve lineer kriptanaliz (Matsui 1994) yöntemleri değişim kutularının diferansiyel ve lineer özelliklerinden faydalandığı için blok şifre tasarımcıları değişim kutularını seçerken fark dağılım tablosu (difference distribution table) ve lineer tahmin tablosu (linear approximation table) değerlerini dikkate alırlar. Bu iki ana kriterin dışında değişim kutularının dallanma sayılarının (branch number, Saarinen 2011) azlığı cebirsel ataklara (Courtois ve Pieprzyk 2002) karşı zayıflık oluşturabileceği gösterilmiş, değişim kutularının kaç paya bölünebileceği (Bilgin vd. 2012) de diferansiyel güç analizi (Kocher vd. 1999) gibi yan kanal saldırılarına karşı güvenlik kriteri olarak kullanılabileceği gösterilmiştir.

Geçen yıl tamamlanan 112E101 kodlu projemizde literatüre kattığımız iki yeni değişim kutusu güvenlik kriteri, blok şifre tasarımcılarının değişim kutusu oluştururken dikkat etmesi gereken başka özelliklerin olduğunu göstermiştir. Rahatsız Edilmemiş Bit (undisturbed bit) ismini verdiğimiz (Tezcan 2014) güvenlik kriteri, değişim kutularındaki bir olasılıklı diferansiyellerin daha iyi kesik diferansiyel (truncated differential, Knudsen 1994), imkansız diferansiyel (impossible differential, Biryukov vd. 2005) ve olası olmayan diferansiyel (improbable differential, Tezcan 2010) ataklara izin verdiği gösterilmiştir. Diferansiyel Faktör (differential factor) ismini verdiğimiz (Tezcan ve Özbudak 2014) ikinci güvenlik kriteri, değişim kutularından önce $\oplus$ (XOR) işlemi uygulanan anahtarın, diğer anahtarlarla bir olasılıkla ilişkili olduğu durumları inceler. Blok şifrelere yapılan istatistiksel ataklarda, doğru anahtarı bulmak için eldeki her seçili düz metin ikilisi olası anahtarlarla kısmi şifreleme işleminden geçirilir (veya önceden şifreleme işlemi yapılıp sonuçlar bir tabloda tutulur ve kısmi şifreleme işlemi yerine tablodan okuma (table lookup) işlemi gerçekleştirilir). Ve eğer şifreleme işlemi sonucunda beklenen istatistiksel özellik gözlemlenirse, o anahtar için tutulan sayaç 1 arttırılır. Dolayısıyla atağın zaman karmaşıklığı düz metin ikilileri ve saldırının yapıldığı anahtar sayısıyla doğru orantılıdır. Örneğin eğer atak anahtarın 50 bitini ele geçirmek için yapılıyorsa, her düz metin ikilisi 2^{50} adet anahtarla kısmi olarak şifrelenir. Diferansiyel faktörlerin varlığı bazı anahtar adayları için tutulan sayacın, diğerleriyle aynı olacağını önceden bilmemizi sağlar. Dolayısıyla atağı gerçekleştirirken bu anahtarlar için şifreleme işlemi yapmamıza gerek yoktur ve bu sayede atağı çok daha az bir zaman karmaşıklığı ile gerçekleştirmek mümkün olmaktadır.

Yakın zamana kadar SERPENT (Biham vd. 1998) şifresine yapılan bilinen en iyi ataklar, Dunkelman vd. (2008)'in şifrenin 10, 11 ve 12 döngülü haline uyguladıkları diferansiyel-lineer

(Langford ve Hellman 1994) ataklardı. Bu ataklar sırasıyla anahtarın 40, 48 ve 160 bitini ele geçirmek üzerinedir ve atakların zaman karmaşıklığı $2^{115.2}$, $2^{135.7}$ ve $2^{249.4}$ kısmi şifreleme işlemi olarak verilmiştir. Fakat yakın zamanda keşfettiğimiz ve ismini diferansiyel faktör (Tezcan Özbudak 2014) olarak koyduğumuz değişim kutuları zayıflıklarıyla bu sayıların yanlış olduğunu gösterdik. Bu zayıflıklar nedeniyle bu atakların anahtarın sadece sırasıyla 38, 46 ve 157 bitini ele geçirebileceğini, dolayısıyla atakların zaman karmaşıklıklarının sırasıyla $2^{113.2}$, $2^{133.7}$ ve $2^{246.4}$ olduğunu gösterdik. Bu elde ettiğimiz yeni ataklar, SERPENT şifresine yapılan bilinen en iyi ataklardır. Yazarların böyle bir durumu gözden kaçırmalarının sebebi yüksek zaman karmaşıklığı nedeniyle bu atakların doğruluğunu kontrol edememiş olmalarındandır. Dolayısıyla yüksek işlem gücüne sahip sistemlerle teoride elde edilen atakların tamamını ya da kısaltılmış hallerini deneysel yollarla doğrulamak son derece önemlidir.

Bu projede sadece bir olasılıkla birbiriyle ilişkili olan anahtarlar yerine, birden daha düşük olasılıklarla da birbiriyle ilişkili olan anahtarları incelemek ana hedeflerimizden ilkidir. Bu sayede genişleteceğimiz Diferansiyel Faktörlere, Sözde Diferansiyel Faktörler (Quasi Differential Factors) ismini verdik. Proje öncesi sözde diferansiyel faktörlerin atakların zaman karmaşıklıklarını daha da düşüreceği öngörülmüştür. Proje sonucunda bu öngörünün doğru olduğu gösterilmiş ve örnek olarak da SERPENT şifresine yapılan atakların zaman karmaşıklıkları 32 kat hızlandırılmıştır.

Teorik olarak elde edilen atakların ve diferansiyellerin deneysel yollarla kontrolünün önemi yakın zamanda PRESENT (Bogdanov vd. 2007) şifresine yaptığımız ataklarda (Tezcan 2014) kendini yeniden göstermiştir. Başka ataklardaki gözlemleri sonucunda Blondeau (2014a), PRESENT şifresi için elde ettiğimiz 13 döngülü atağın pratikte çalışmayacağını deneysel sonuçlar elde etmeden iddia etmiştir. Blondeau'nun deneysel yollarla kontrol yapmamasının sebebi bu tarz bir deneyin bilgisayar işlemcilerinde çok uzun sürecek olmasıdır. Buna karşılık olarak ekran kartlarının paralel işlem gücünü kullanarak tek bir NVIDIA Tesla k20 ekran kartıyla 2^{45} adet 8 döngülü PRESENT şifreleme işleminin 8 saatten kısa bir sürede yapılabileceğini gösterip, bu atağın doğruluğunu deneysel olarak gösterdik (Tezcan ve Temizel 2014). Bu deneyi tek bir işlemci çekirdeğiyle yapmak yaklaşık 13 gün sürmektedir. Bizim deney sonuçlarımızın üzerine kendi deneyini tamamlayan Blondeau da atağımızın doğruluğunu kabul etmiştir (Blondeau 2014b).

Ekran kartlarının paralel işlemlerdeki başarısı mimarilerinden kaynaklanmaktadır. Günümüz teknolojisinde üst seviyedeki işlemciler genellikle 4 çekirdeklidir ve bu çekirdekler en fazla 4.0 GHz hızındadırlar. Ekran kartları ise düşük hızlarda ama çok daha fazla çekirdeğe sahiptirler.

Örneğin bu proje kapsamında oluşturduğumuz masaüstü bilgisayarda kullandığımız 3 adet GTX 970 ekran kartının her biri 1253 MHz'de 1664 çekirdeğe sahiptir. Ekran kartlarının dezavantajı ise bu çekirdeklerin hepsinin aynı komutu uygulamak zorunda olmasıdır. Bu aynı komutu farklı verilere uygulamak mümkün olduğu için paralel işlemler ekran kartlarında çok iyi sonuçlar vermektedir.

Projenin ikinci temel amacı ekran kartlarının bu paralel işlemlerdeki gücünü şifreleme algoritmalarında kullanarak elde edilecek hızlanmayı ve güvenlik sınırlarını belirlemektir. Elde etiğimiz sonuçlar, ekran kartlarının AES-NI gibi donanımsal olarak AES şifrelemesi yapabilen işlemcilerden bile daha hızlı olduğunu göstermiştir. Ayrıca 80 bitlik ya da daha kısa anahtar kullanan algoritmaların artık güvenli olmadığı ve kullanılmamaları gerektiği gösterilmiştir.

5.3 Gereç ve Yöntem

Proje için değişim kutularının kriptografik özelliklerini analiz eden yazılımın yanı sıra daha iyi değişim kutularının aranmasını sağlayacak bir yazılım da üretilmiştir. Ekran kartlarına optimize edilecek şifreleme algoritmaları öncelikle CPU için C dilinde sonra da ekran kartları için CUDA dilinde yazılmıştır.

Proje kapsamında ekran kartlarının paralel işlem gücünün kriptografi alanında kullanılması planlanmış ve bu kapsamda proje için 3 adet Nvidia GTX 970 ekran kartına sahip bir bilgisayar oluşturulmuştur. Proje önerisi verildiğinde GTX 970 ekran kartları henüz üretilmemiş olduğu için ilk başta 4 adet GTX 960 ekran kartının kullanılması planlanmıştır. Proje başladıktan sonra mevcut 4 adet ekran kartı takılabilen anakartların maliyetinin fazla olması nedeniyle 3 ekran kartlı bir sistem daha uygun görülmüştür. 3 adet GTX 970 ekran kartının 4 adet GTX 960 ekran kartından daha hızlı olması ve daha az enerji tüketmesi nedeniyle bu şekilde oluşturduğumuz sistem her açıdan daha iyi olmuştur. Bu makinenin ısınma ve performans açısından testleri yapılmış ve projede aktif olarak kullanımına başlanmıştır. Tükettiği enerjinin kullanılan güç kaynağına herhangi bir zarar vermediği gözlemlenmiştir. 3 ekran kartı da tam performans çalıştığında 80 santigrat derecenin üstüne çıkmamaktadır. Ayrıca kullandığımız GPU Tweak yazılımı sayesinde bu kartları 75 derecenin altında çalışmaya zorlayarak kartların ömrünü yıllarca uzatmış bulunmaktayız. Proje süresince ekran kartları analizleri bu cihaz kullanılarak yapılmıştır.

5.3.1 S-box Analyzer

Bu yazılım değişim kutularının kriptografik özelliklerini analiz etmek amacıyla hazırlanmıştır. 3x3, 4x4, 5x5, 6x6, 7x7, 8x8 ve 9x9 ebatlarındaki değişim kutularının aşağıdaki özelliklerini ölçmektedir:

1. Diferansiyel dağılım tablosu (DDT)
2. Lineer yapılar (linear structures)
3. Rahatsız edilmemiş bitler (undisturbed bits)
4. Otokorelasyon tablosu (Autocorrelation table)
5. Diferansiyel faktörler
6. Sözde diferansiyel faktör tablosu

Eğer 3x3 değişim kutuları incelenmek istenirse, toplamda sadece 40320 adet birebir ve örten 3x3 değişim kutusu olduğu için yazılım bütün hepsini analiz edip sonuçları çıktı dosyasına kaydetmektedir. Diğer ebatlardaki değişim kutuları için kullanıcıların girdiği değişim kutuları analiz edilmektedir. Literatürdeki bütün blok şifre, akan şifre ve özet fonksiyonu algoritmalarını tarayarak içerdikleri değişim kutularını yazılımın içine ekledik. Yazılımın son halinde mevcut kriptosistemlerde kullanılan 3 adet 3x3, 141 adet 4x4, 2 adet 5x5, 3 adet 6x6, 2 adet 7x7, 33 adet 8x8 ve 2 adet 9x9 farklı değişim kutusu mevcuttur.

5.3.2 APN Search

Diferansiyel dağılım tablosu (DDT) diferansiyel kriptanaliz ve benzeri ataklara olan güvenliği belirlemek için kullanılan iyi bir ölçüttür. Bu tablo iki girdi arasındaki bit farkının çıktıda oluşturduğu farkı saydığı için, istatistiksel olarak bu tablodaki değerlerin küçük olması tasarımcıların önceliğidir. Tablo bütün girdi ikililerini değerlendirdiği için ve (a,b) ikilisi ile (b,a) ikilisi aynı bit farkına sahip olduğu için tablodaki bütün değerler çift olmak zorundadır. Dolayısıyla en ideal değişim kutusunun DDT'sinde sadece 0 ve 2 sayısını görmemiz gerekir. Bu şekildeki değişim kutularına neredeyse mükemmel lineer olmayan (almost perfect nonlinear APN) değişim kutusu adı verilmiştir. 5x5 ya da 7x7 gidi tek ebatlı değişim kutuları için bu tarz değişim kutularının nasıl elde edilebileceğini gösteren matematiksel oluşturma yöntemleri mevcuttur. 4x4 ebatları için ise APN özelliğine sahip bir değişim kutusu olmadığı değişim kutularının afin denklik sınıfları kullanılarak gösterilmiştir. Dolayısıyla 6x6 ya da 8x8 gibi çift boyutlardaki değişim kutularının APN özelliğine sahip olup olamayacağı uzun bir süre açık bir

problem olarak kalmıştır. Dillon (Browning vd. 2010) matematiksel yöntemler kullanarak APN özellikli bir 6x6 ebatında değişim kutusu bulmuş ama daha başkaları henüz bulunamamıştır.

Bu yazılımda diferansiyel faktörlerin DDT ile ilişkileri kullanılarak değişim kutusu uzayını daha hızlı taramak mümkündür. Bu sayede 4x4 değişim kutularının hepsi taranarak APN özellikli 4x4 değişim kutusu olmadığı gösterilmiştir. 6x6 ya da 8x8 ebatlarındaki değişim kutuları sayısı çok fazla olduğu için hepsini bu yazılımla taramak mümkün değildir. Bu yüzden bu yazılım ile uzayın belirli bir kısmını taramak mümkündür ve bu özelliği kullanarak Dillon'ın 6x6'lık APN değişim kutusu ve ona eşdeğer 31 farklı değişim kutusu daha bulunmuştur. Yaptığımız taramalar sırasında Dillon'ın değişim kutusuna afin denk olmayan başka bir değişim kutusu ya da APN özellikli 8x8 değişim kutusu henüz bulunamamıştır.

5.3.3 Block Cipher Suite

Proje süresince bazı teorik atakların pratikteki doğruluğunu kontrol etmek için ve blok şifrelerin ekran kartlarındaki performansını ölçmek için bazı blok şifrelerin CPU ve GPU için optimizasyonları yapılmıştır. Kodları yazılan şifreler şu şekildedir:

1. A5/1
2. AES
3. ASCON
4. CRYPTO1
5. DES/3DES
6. PRESENT
7. RECTANGLE
8. SERPENT
9. SKIPJACK

Kodların kullanımı için "*115E447 Kaynak Kodları ve Kullanıcı Kılavuzu*" başlıklı bir doküman hazırlanmıştır. HIGHT, CLEFIA, Camellia, SEED, MISTY1, CAST-128 ve KASUMI şifreleri de incelenmiş ama tablo tabanlı kodlama tekniğine çok müsait olmadıkları için ekran kartlarından gelecek hızlanma diğer şifrelerdeki kadar olmayacağı için ekran kartlarına optimizasyonu yapılmamıştır.

5.4 Bulgular

1. Sözde diferansiyel faktörlerin geliştirilmesi: Öncelikle diferansiyel faktörler teorisi daha detaylıca incelenmiştir. Diferansiyel faktörlerin, diferansiyel atakların zaman karmaşıklığını azaltmanın yanı sıra, bu atakların veri ve hafıza karmaşıklığını da azaltabildiği gösterilmiştir. Bu gözlemler kullanılarak SERPENT şifresine yaptığımız bir önceki atakların veri ve zaman karmaşıklıkları daha da iyileştirilmiştir.

Diferansiyel ataklar genelde iki aşamadan oluşur: Diferansiyel kullanılarak bazı anahtar bitlerinin elde edildiği anahtar tahmin aşaması ve geriye kalan anahtar bitlerinin tek tek denenerek elde edildiği kaba kuvvet aşaması. Araştırmalarımız sırasında diferansiyel faktörlerin ilk aşamanın zaman karmaşıklığını azalttığı ama ikinci aşamanın zaman karmaşıklığını arttırdığını gösterdik. Bu nedenle ilk aşamanın daha fazla zaman karmaşıklığı gerektirdiği ataklar diferansiyel faktörler kullanılarak iyileştirilebilir. İkinci aşamanın daha fazla zaman karmaşıklığı gerektirdiği ataklar eğer diferansiyel faktör içeriyorsa, bu ataklar gerçekte daha fazla gayrete ihtiyaç duymaktadır ve atağın işe yarayabilmesi için düzeltilmesi gerekmektedir. SERPENT şifresine yaptığımız ataklar bu ilk kategoriye girdiği için daha da geliştirilmiştir. Bunun yanında, literatürde Wang (2008) tarafından PRESENT şifresine yapılan diferansiyel atağın ikinci kategoriye girdiği gözlemlenmiş ve gerçekte bu atağın 64 kat daha fazla gayret gerektirdiği gösterilerek bu atak düzeltilmiştir. Bu ana kadarki anlatılan yeni elde edilmiş teoremler, iyileştirilmiş SERPENT atağı ve düzeltilmiş PRESENT atağı makale olarak Lightsec 2015 konferansına kabul almış ve Almanya'da sunulmuştur. Makalenin başlığı "Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT" şeklindedir.

Ayrıca diferansiyel faktörler şu ana kadar sadece diferansiyelin bir üst ya da alt döngüsünde yer aldığı zaman diferansiyel ataklara etkili olduğu gözlemlenmişken, çalışmalarımız sırasında diferansiyel faktörlerin 3 farklı gruba ayrılabileceği gösterilmiştir. Bu 3 grubun yapısı incelenerek diferansiyelin bir üst ya da alt döngüsü dışındaki döngülerdeki diferansiyel faktörlerin atağa ne tür etkileri olduğu gösterilmiştir.

Diferansiyel faktör teorisini geliştirdikten sonra sözde diferansiyel faktörlere genişletilmesi araştırılmış ve bu yeni özelliğin diferansiyel ataklarda ne şekilde kullanılabileceği incelenmiştir. Beklendiği üzere sözde diferansiyel faktörlerin diferansiyel atakların zaman karmaşıklığını azalttığı gösterilmiştir. "Quasi-Differential Factors: Improved Differential Attacks on SERPENT" başlığıyla bir dokumanda çalışmalarımız toplanmıştır ve dokumanın bütününün ya da iki parçaya bölünmüş halinin uluslararası dergilere yollanması planlanmaktadır.

2. Literatürdeki atakların sözde diferansiyel faktörler yardımıyla geliştirilmesi: Geliştirilen diferansiyel faktörler teorisinin, SERPENT şifresine yapılan ve bu şifreye uygulanmış bilinen en iyi ataklar olan diferansiyel-lineer ataklara olan etkisi incelenmiştir. Bu sayede bilinen en iyi atağın 8 kat daha hızlı yapılabileceği gösterilmiştir. Bu sonuçlar yukarıda bahsettiğimiz Lightsec 2015 konferansı makalemizde yer almıştır. Sözde diferansiyel faktörler teorisini geliştirmemiz daha önceden yaklaşık 8 kat hızlandırdığımız SERPENT şifresine yapılan bilinen en iyi atakların zaman karmaşıklıklarını ek olarak 32 kat daha hızlandırmıştır. Bu en hızlı ataklar "Quasi-Differential Factors: Improved Differential Attacks on SERPENT" dokümanımızda mevcuttur.

Bunun yanı sıra hafif blok şifreler olan PRESENT, PRIDE ve RECTANGLE şifrelerine literatürde verilmiş olan diferansiyel ataklar incelenmiştir. PRESENT ve RECTANGLE'a olan ataklar geliştirilmiş, PRIDE'a verilen ataklar düzeltilmiştir. Bu 3 şifreye yaptığımız ataklar Lightsec 2016 konferansında sunulmak üzere kabul almış ve sunulmuştur. Makalenin başlığı "Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited" şeklindedir.

Bunlara ek olarak CRYPTON, DES, FOX, GOST, HISEC, JOLTIK, KHUDRA, LBLOCK, LAC, LED, LUFFA, MIDORI, NOEKEON, Piccolo, PROST, QTL, ROADRUNNER, SAFER, SARMAL, SPONGENT, Twofish algoritmaları ve değişim kutuları diferansiyel faktörler açısından incelenmiştir. Literatürdeki ataklar incelenerek bazılarının çok küçük miktarda hızlandırılabileceği gösterilmiştir. FOX ve SAFER gibi 8x8 boyutunda değişim kutusu olan blok şifrelerin diferansiyel faktör içerdiği gösterilmiş ve bu sayede büyük boyutlardaki değişim kutularının da diferansiyel faktörlerden etkilendiği gösterilmiştir. Bu elde ettiğimiz sonuçlar "On Differential Factors" başlığıyla ISCTURKEY konferansına makale olarak kabul almış ve sunulmuştur.

3. Yeni atakların elde edilmesi: Şu an devam etmekte olan ve "authenticated encryption" (kimlik denetimli şifreleme) algoritmalarının yarıştığı CAESAR yarışmasındaki algoritmalar proje konumuz olan değişim kutuları zayıflıkları açışından incelenmiştir. Bu zayıflıklar kullanılarak ASCON algoritmasına bilinen en iyi truncated, impossible ve improbable diferansiyel ataklar verilmiştir. Bu ataklar sayesinde algoritmanın kriptografi camiası tarafından analizi daha iyi şekilde yapılmış ve Ağustos ayında açıklanan yarışmanın ilk 15'ine kalmasına katkı sağlamıştır. Elde ettiğimiz bu ataklar ICISSP 2016 konferansında Roma'da makale olarak sunulmuştur. Makale başlığı "Truncated, Impossible, and Improbable Differential Analysis of ASCON" şeklindedir. Ayrıca bu yarışmadaki diğer şifrelerden Joltic, Ketje, LAC ve Prost

şifrelerinin değişim kutularının da diferansiyel faktör içerdiği gözlemlenmiş ama çalışmalarımız sonucu yeni ataklar elde edilememiştir.

4. Blok şifrelerin ekran kartlarına optimizasyonu: Proje kapsamında ekran kartlarının paralel işlem gücünün kriptografi alanında kullanılması planlanmış ve bu kapsamda proje için 3 adet Nvidia GTX 970 ekran kartına sahip bir bilgisayar oluşturulmuştur. Bu makinenin ısınma ve performans açısından testleri yapılmış ve projede aktif olarak kullanımına başlanmıştır.

Öncelikle AES, DES, 3DES, PRESENT, SERPENT, SKIPJACK gibi algoritmaların CPU kodları yazılmış ve optimizasyonu elde edilmiştir. Sonra da AES, PRESENT, DES, 3DES ve SERPENT blok şifrelerinin ekran kartı optimizasyonu yapılmış ve literatürdeki en hızlı çalışan kodlar elde edilmiştir. Tek tek yazılan bu CPU kodları "Block Ciphers on CPU" isimli bir yazılımda, GPU kodları ise "Block Ciphers on GPU" isimli bir yazılımda toplanmıştır. Fakat daha iyi analiz ve değişiklikler için bütün şifrelerin kaynak kodları ayrı yazılımlar olarak da hazırlanmış ve daha iyi performans ölçümleri elde edebilmek için bu bağımsız yazılımlar kullanılmıştır. Bütün kaynak kodlar "*115E447 Kaynak Kodları ve Kullanıcı Kılavuzu*" dokümanında yer almaktadır.

ODTÜ Bilgi İşlem Dairesinin, akıllı kart özelliğine de sahip olan ODTÜ kimliklerinin kriptografik açıdan ne kadar güvenli olduğunu kontrol etmemizi istemesi üzerine NXP firması tarafından üretilen ve ODTÜ kimliklerinde kullanılan MIFARE Classic 1k akıllı kartlarını da analiz etmiş bulunuyoruz. Bu kartlarda kullanılan 48 bit anahtara sahip CRYPTO1 şifresi ekran kartları kullanılarak kırılmaya müsaittir. Bunun için kart ile 1 saniyeden kısa süre etkileşime geçmek gerekmektedir. Bu iş için kullanılacak standart antenler 3-10 santimetreden kart ile haberleşebileceği için, kart sahibinin yanında geçmek gerekli veriyi almak için yeterlidir. Garcia vd. (2008) daha sonra bu veriye kaba kuvvet türü ataklar yapılabileceğini göstermiş ve Chih vd. (2010) bu atağın tek bir Nvidia GTX 280 ekran kartı ile yaklaşık 10 gün süreceğini göstermişlerdir. Birçok optimizasyon tekniği ve bitsliced kodlama yöntemi kullanarak biz bu atağı Nvidia GTX 970 ekran kartında 5 saatten kısa bir sürede gerçekleştirebilir hale geldik. Sonuçlar Tablo 1'de gösterilmiştir.

Tablo 1. Dizüstü ve masaüstü bilgisayar ekran kartları ile ODTÜ kimlik kartlarında da kullanılan MIFARE Classic 1k çiplerindeki CRYPTO1 şifresinin 48 bitlik bir anahtarını ele geçirmek için gereken süre

	GTX 860M	**GTX 970**
Çekirdek Sayısı	640	1664
İşlemci Hızı	1024 MHz	1253 MHz
Saniyede denenen anahtar sayısı	6673 milyon	15575 milyon
Atak süresi	11,7 saat	5 saat

Dolayısıyla proje için oluşturduğumuz bilgisayar ile ODTÜ kimlik kartlarını 1,5 saatte kopyalamamız mümkündür. ODTÜ kimlik kartları yemekhane gibi yerlerde ödeme yapmak için kullanıldığı gibi, birçok bina ve laboratuvarın kapısını açmak için de kullanılmaktadır. Dolayısıyla bu kartlar ciddi bir güvenlik zafiyeti oluşturmaktadır. Çözüm önerilerimizi de içeren raporumuz GİZLİ ibaresiyle rektörlüğe ulaştırılacaktır.

Ekran kartlarının gücünü kullanarak bir de Türkiye'deki GSM güvenliğini kontrol ettik. Halen A5/1 şifresinin kullanıldığı görüşmeleri dinlemek için 64 bit anahtar kullanan bu algoritma için Rainbow tabloları ismiyle bilinen tabloları oluşturmak gerekmektedir. Bunun için de en az 2^{64} adet şifreleme işlemi yapmak gerekmektedir. Sonuçta elde edilecek tabloları 1 ya da 2 terabyte'lık bir disk'e kaydedip görüşme yapan kişinin 150 metre kadar yakınına gelerek görüşmeleri dinlemek mümkündür. Yazdığımız kodların performansı Tablo 2'te gösterilmiştir.

Tablo 2. İşlemci ve ekran kartlarının A5/1 şifreleme işlemi performansı

İşlemci	**Performans**
Intel i7-4702QM (CPU)	2^{22} şifreleme/saniye
Nvidia GTX 860M (GPU)	2^{28} şifreleme/saniye
Nvidia GTX 970 (GPU)	2^{32} şifreleme/saniye

Dolayısıyla birkaç ekran kartına sahip kişiler bu kartları birkaç ay çalıştırılarak GSM görüşmelerini belli bir olasılıkla dinlemeye yarayacak tabloları oluşturabilirler. Burada dikkat edilmesi gereken konu, küçük miktarda tablo oluşturarak yüzde bir ihtimalle çalışan bir saldırı elde etmek bile ciddi bir tehlikedir çünkü bu her 100 görüşmeden 1 tanesini dinleyebilmek anlamına gelmektedir. Biz projemizde sadece performans testi yaptık ve herhangi bir tablo oluşturmadık. Fakat bu tabloları internetten elde edilecek kodlarla oluşturmak zor olmadığı gibi, tabloların hazır haline de ulaşmak mümkündür. Dolayısıyla Türkiye'deki GSM operatörlerinin

hızla 3G standardı olan KASUMI blok şifresine geçmeleri kişisel mahremiyet açısından tavsiye edilmektedir.

AES algoritması birkaç yıl önce INTEL işlemcilere AES-NI ismiyle donanımsal olarak eklenmiş ve yazılım performanslarının çok üzerinde AES şifrelemesi sağlanmıştır. Bu projede optimizasyonunu yaptığımız AES ekran kartı kodları AES-NI'dan çok daha hızlıdır. Bu sayede tüm disk şifrelemesi ya da dosya şifrelemesi gibi operasyonları ekran kartlarıyla yapmak daha hızlı olacaktır ve bu süreç boyunca işlemci hiç kullanılmayacaktır. Bu AES kodlarının ticari değeri vardır.

Dosya şifrelemesi için GPU'da elde ettiğimiz AES hızı, AES-NI hızından 2,5 kat daha hızlı olsa da, kaba kuvvet saldırıları yaparken elde ettiğimiz hız çok daha fazladır. Bunun nedeni AES-NI kodları standart AES kodlarından daha hızlı olmasına rağmen, kaba kuvvet ataklarında her anahtar için yinelenen anahtar genişletme algoritması (key expansion) bu kodlarda yavaşlamaya neden olmasıdır. Kaba kuvvet saldırılarına yönelik 4 çekirdekli güncel bir CPU ile projede kullandığımız bir adet GTX 970 GPU'su için elde ettiğimiz sonuçları AES ve PRESENT şifreleri için şöyle gösterebiliriz:

Tablo 3. İşlemci ve ekran kartlarının AES şifresine yapılan kaba kuvvet ataklarındaki performansı

AES	CPU	CPU (AES-NI)	GPU
1 saniyede denenen anahtar sayısı	32.904.567	90.426.075	1.180.260.318

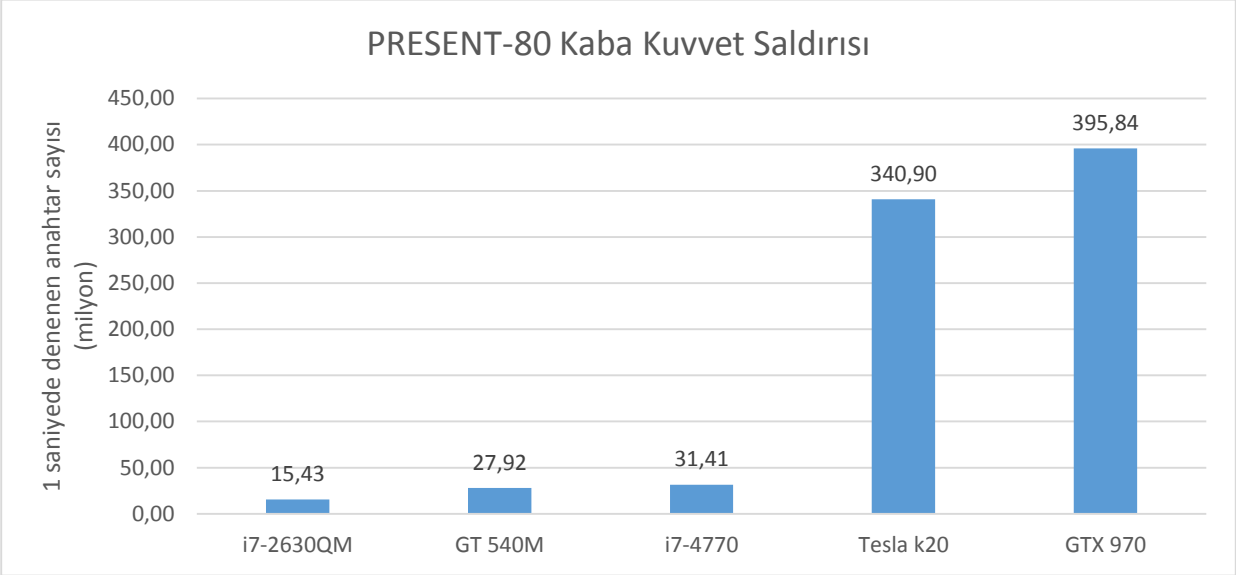
Tablo 4. İşlemci ve ekran kartlarının PRESENT şifresine yapılan kaba kuvvet ataklarındaki performansı

PRESENT	CPU	GPU
1 saniyede denenen anahtar sayısı	25.811.102	395.840.383

Dolayısıyla AES anahtarına yapılacak kaba kuvvet ataklarını 13 kat, PRESENT anahtarına yapılacak kaba kuvvet ataklarını ise 12,6 kat hızlandırmış durumdayız.

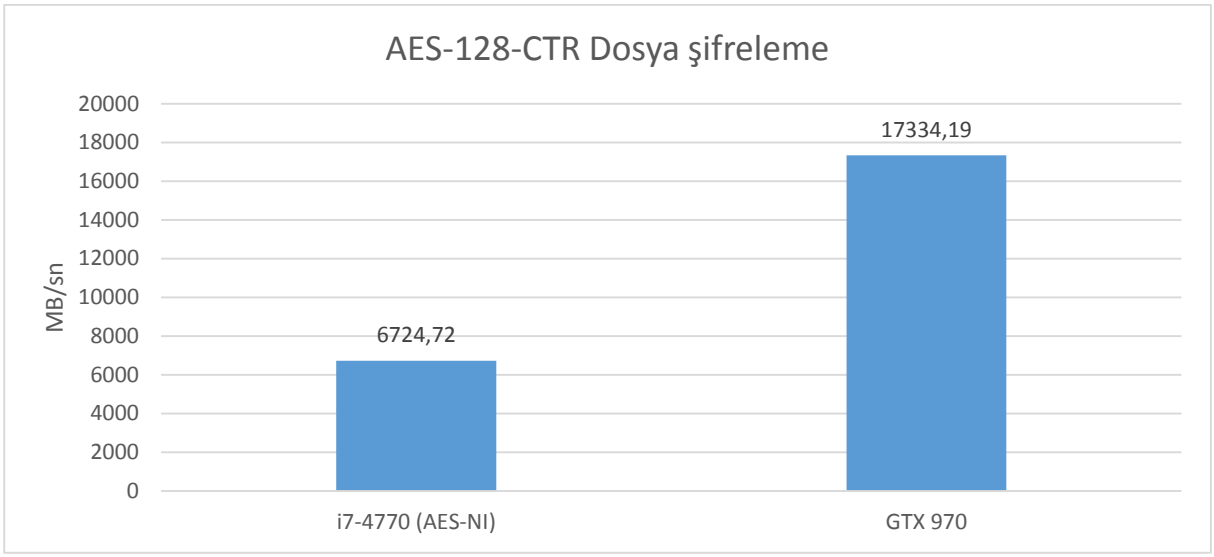
80 bitlik PRESENT şifresi için elde ettiğimiz performans sonuçları Şekil 1'de gösterilmiştir. Bu sonuçlar ve 48 bitlik CRYPTO1 şifresi ve 64 bitlik A5/1 şifresi için elde ettiğimiz sonuçlar, 80 bit ve daha kısa anahtar kullanan algoritmaların gerçek hayatta hiçbir güvenlik sağlamadığının

göstergesidir. Dolayısıyla 128 bitten daha kısa olan anahtarlar kriptografik algoritmalarda kullanılmamalıdır.



Şekil 1. Dizüstü ve masaüstü bilgisayar işlemci ve ekran kartlarının 80 bit anahtarlı PRESENT şifresine yapılan kaba kuvvet ataklarındaki performansı

Kaba kuvvet ataklarında her seferinde yeni bir anahtarla şifreleme işlemi yapıldığı için, anahtar genişletme algoritmasını da kullanmak gerekmektedir. Ama dosya ya da disk şifreleme gibi gündelik kullanımlarda bütün şifreleme işlemleri tek bir anahtarla yapılacağı için performans kriteri, saniyede kaç megabyte (MB) şifrelendiği şeklinde olmalıdır. AES şifresini 128 bitlik anahtar kullanarak sayaç (CTR) modunda çalıştırarak güncel bir 4 çekirdekli i7 işlemci ile yaptığımız kıyaslama aşağıdaki şekilde verilmiştir. Görüldüğü üzere ekran kartında elde ettiğimiz performans Intel'in AES-NI donanım komutlarından 2,5 kat daha hızlıdır. Eğer 8 çekirdekli çok daha modern bir işlemci kullanılsaydı bile GTX 970 ekran kartının performansına yetişemeyecekti. Fiyat performans olarak da düşünüldüğünde 8 çekirdeğe sahip Intel işlemciler raporun yazıldığı sırada 1350$'dan daha pahalıdır. Bunun yanı sıra GTX 970 ekran kartları ise 250-300'dır.



Şekil 2. 4 çekirdekli i7 işlemci ile Nvidia GTX 970 ekran kartının sayaç modunda 128 bit anahtarlı AES ile dosya şifreleme performansları kıyaslaması

DES ve PRESENT için elde ettiğimiz ekran kartı hızları, CPU'ların çok ilerisindedir. COPACOBANA ve RIVYERA gibi FPGA tabanlı sistemlerin performanslarıyla kıyasladığımızda ise fiyat/performans oranı olarak ekran kartlarının bu sistemleri yakaladığını görmekteyiz.

AES için elde ettiğimiz sonuçlar ise CPU ve AES-NI gibi donanımsal yonga seti içeren Intel işlemcilerin çok ilerisindedir. Ayrıca elde ettiğimiz ekran kartı sonuçları fiyat/performans oranı olarak COPACOBANA ve RIVYERA gibi FPGA tabanlı sistemlerden çok daha iyidir. Dolayısıyla FPGA'lerin her zaman GPU'lardan daha hızlı olduğu düşüncesi doğru değildir.

5. Atakların ve diferansiyellerin ekran kartlarında doğrulanması: Dunkelman vd. tarafından SERPENT için bulunan 11 döngülü diferansiyel-lineer yolun ilk 3 döngüsü diferansiyel, son 8 döngüsü lineer bir ilişki içermektedir. Yazarlar bu iki farklı metodun birbiriyle beklenenden daha iyi karıştığını göstermek için ilk 4 döngüsünün 2^{-15} olması gereken teorik olasılığının pratikte $2^{-13.75}$ olduğunu işlemciler kullanılarak deneylerle göstermiştir. İşlem güçleri daha fazla döngüyü kontrol etmeye yetmediği için daha uzun döngülerin olasılığını kontrol edememişlerdir. Bu nedenle elde edilen $2^{1.25}$'lik iyileşmenin sonraki döngülere de yansıdığı varsayılmış ama bu varsayımın doğruluğu bilimsel olarak gösterilememiştir.

Bu projede elde ettiğimiz ekran kartı optimizasyon kodları ile SERPENT için bulunan bu yolun ilk defa 5 döngüsünün olasılığı da deneylerle kontrol edilmiş ve bu olasılığın Dunkelman vd. varsaydığı gibi $2^{-17.75}$ değil $2^{-17.63}$ olduğu gösterilmiştir. Dolayısıyla Dunkelman vd.'lerinin

varsayım sonucu verdikleri atağın gerçekte mümkün olduğu gösterilmiş ve gerçek olasılığın Dunkelman vd.'lerinin varsayımından daha da iyi olduğu elde edilmiştir. Elde edilen hız kazanımı $2^{0.12}$'dir. Ekran kartlarının güçleri kullanılarak 6 döngülük kısımı kontrol etmek için 2^{59} adet 6 döngülük SERPENT şifreleme işlemi uygulanmış ve elde edilen bu kazanımın 6 döngüye de aktarıldığı gözlemlenmiştir. 2^{59} adet şifreleme işlemini ekran kartları yerine son model tek bir işlemci ile yapmak 15 yıldan fazla sürecekken, biz bu sonuçları 3 ekran kartı içeren sistemimiz ile 5 ay içerisinde elde etmiş bulunuyoruz.

5.5 Yayınlar

Proje süresince toplamda 11 doküman hazırlanmıştır. Bunlardan 3 tanesi proje bitiminde tamamlanmış ve içerikleri makale olarak yayınlanmaları için yollanacak dokümanlar, 3 tanesi güvenlik nedeniyle yakın zamanda yayınlanması planlanmayan çalışma ve raporlar, 5 tanesi ise yayınlanmış makalelerdir. Ayrıca proje bursiyeri Merve Öğünç ve Siber Güvenlik Bölümü öğrencileri Erol Doğan ve Asuman Şenol'un proje konusuyla ilgili yüksek lisans tezlerinin 2017 yılı içerisinde tamamlanması beklenmektedir.

Yayınlanması beklenen çalışmalar:

1. **Quasi-Differential Factors: Improved Differential-Linear Attacks on Serpent:** Bu doküman projenin temel amacı olan sözde diferansiyel faktörlerle ilgili teoriyi içermektedir. Ayrıca diferansiyel faktörlerin sınıflandırılması yapılmış ve sözde diferansiyel faktörler kullanılarak SERPENT şifresine yapılan en iyi ataklar 32 kat hızlandırılmıştır. *01_sozdediff.pdf* dosya ismiyle yüklenen bu dokümanın içeriğinden 1 ya da 2 makalenin ilgili dergi ve konferanslara yollanması hedeflenmektedir.
2. **High Performance Cryptanalysis on Graphics Processing Units:** Bu doküman proje süresince ekran kartlarına optimize ettiğimiz şifrelerin performanslarını ve güvenlik üzerine etkilerini özetlemektedir. *02_GPU.pdf* dosya ismiyle yüklenen bu dokümanın içeriğinden 1 ya da 2 makalenin ilgili dergi ve konferanslara yollanması hedeflenmektedir.
3. **Modified Differential Cryptanalysis on LBlock using Differentail Factors:** Bu doküman LBLOCK şifresine yapılan diferansiyel atakların diferansiyel faktörler yardımıyla nasıl hızlandırılabileceğini anlatmaktadır. *03_LBLOCK.pdf* dosya ismiyle yüklenen bu dokümanın 7-8 Kasım 2017 tarihinde düzenlenecek ISCTURKEY 2017 konferansına yollanması hedeflenmektedir.

4. Proje bursiyeri Merve Öğünç'ün ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Bölümü'nde Doç. Dr. Ali Doğanaksoy'un danışmanlığında yazmakta olduğu "Differential Cryptanalysis on LBLOCK by Using Differential Factors" başlıklı yüksek lisans tezinin 2017 bahar döneminde tamamlanması beklenmektedir. ODTÜ Enformatik Enstitüsü Siber Güvenlik Bölümü öğrencileri Erol Doğan ve Asuman Şenol'un "Differential Factors and Differential Cryptanalysis of Block Cipher PRIDE" ve "Improved Differential Attacks on RECTANGLE" başlıklı tezlerinin 2017 yılında tamamlanması beklenmektedir. Bu tezlerin yardımcı danışmanlığını Dr. Cihangir Tezcan yapmaktadır.

Güvenlik nedeniyle yakın zamanda yayınlanması planlanmayan çalışmalar ve raporlar:

1. **ODTÜ Akıllı Kartlarının Güvenliği:** Bu çalışmada Mifare Classic 1k akıllı kartlarını kullanan ODTÜ kimlik kartlarının kopyalanmaya karşı olan zafiyetlerini göstermekte ve bu proje kapsamında oluşturduğumuz 3 adet GTX 970 ekran kartına sahip bilgisayarımızda ODTÜ kimlik kartlarını 2 saatten daha kısa bir sürede kopyalayabildiğimizi göstermekteyiz. ODTÜ kimlik kartları yemekhane gibi yerlerde ödemeler için kullanıldığı gibi, birçok bina ve oda/laboratuvar kapılarını açmak için kullanılmaktadır. Bu nedenle kartların kopyalanması ciddi bir güvenlik açığı oluşturmaktadır. Bu çalışmada mevcut kart okuyucuları değiştirmeden sadece kartların değişeceği maddi olarak ucuz olacak çözüm önerilerimizi sunmaktayız. Rektörlüğe GİZLİ ibareli olarak sunulacak bu rapor güvenlik zafiyetleri oluşturmaması için mevcut kartlar değiştirilene kadar yayınlanmayacaktır. Bu doküman *04_odtu_akillikart.pdf* dosya ismiyle yüklenmiştir.

2. **A5/1 Şifresinin ve Türkiye'deki GSM Görüşmelerinin Kaba Kuvvet Saldırılarına Karşı Güvenliği**: Bu çalışmada GSM görüşmelerinin şifrelenmesinde kullanılan 64 bit anahtara sahip A5/1 şifresinin kaba kuvvet ve zaman/hafıza dengeleme ataklarına karşı olan güvenliği incelenmiştir. İncelememiz sonucunda 1 ay içerisinde 2^{64} A5/1 anahtardizini üretme işlemi yaparak Rainbow tablolarını oluşturmak için 2^{21} adet CPU'ya ya da 2^{11} GPU'ya ihtiyaç olduğu gözlemlenmiştir. Dolayısıyla birçok ekran kartına sahip sistemi olanlar bu ekran kartlarını aylarca çalıştırarak oluşturacakları tablolar ile birçok GSM görüşmesini dinlemeleri mümkün olacaktır. Kullanıcıların bu hukuk dışı davranışa maruz kalmamaları için GSM operatörlerinin 128 bit anahtar kullanan ve 3G standardı olan KASUMI blok şifresini varsayılan şifreleme algoritması

olarak belirlemelerini tavsiye etmekteyiz. Bu doküman *05_A51_GSM.pdf* dosya ismiyle yüklenmiştir.

3. **115E447 Projesi Kaynak Kodları ve Kullanıcı Kılavuzu**: Akademik çalışmalar için kullanılan kaynak kodların açık olarak paylaşılması genel düşüncemizdir. Fakat bu proje süresince ürettiğimiz birçok kod, mevcut kullanılan şifreleme algoritmalarının kırılmasını kolaylaştırdığı için bu kaynak kodları ve kodların nasıl kullanılacağını açıklayan kullanıcı kılavuzunu internette paylaşmayı uygun görmüyoruz. Bu doküman, kaynak kodlar ve yazılımların tümü yeni akademik sonuçların elde edilebilmesi için herkesin erişimine açık olmayan ODTÜ Kriptoloji Bölümü Kriptoloji Laboratuvarı ve ODTÜ Siber Güvenlik Bölümü CYDES Laboratuvarında mevcuttur. Bu sayede yeni güvenlik zafiyetleri oluşturmamak ve akademik ilerleme sağlayabilmek için sadece bu alanda çalışan belirli araştırmacılar ve yüksek lisans/doktora öğrencilerinin bu yazılımları kullanmalarına izin verilmiştir. Bu doküman *06_ yazilim_kullanim_kilavuzu.pdf* dosya ismiyle yüklenmiştir. Ayrıca kaynak kod dosyaları *kaynak_kodlar.zip* dosyasında toplanmıştır. Elde edilen kodların paylaşılması güvenlik zafiyetlerine yol açmayacağı bir tarihe gelindiği düşünüldüğü zaman, CRYPTO1 ve AES için elde ettiğimiz ve bildiğimiz kadarıyla bu şifreler için bilinen en hızlı kodlar olan bu kodları Elsevier'in SoftwareX dergisine yollamayı planlıyoruz.

Proje süresince 5 makalemiz yayınlanmıştır (Tezcan 2015; Tezcan 2016; Tezcan vd. 2016a; Tezcan vd. 2016b; Tezcan 2017). Yayınlanan çalışmalar:

1. **Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT**: Bu çalışmamızda Wang (2008) tarafından elde edilen PRESENT şifresi için bilinen en iyi diferansiyel atağın diferansiyel faktörler hesaba katılmadığı için yanlış olduğu gösterilmiş ve düzeltilmiştir. Diferansiyel faktörlerin zaman karmaşıklığının yanı sıra, veri ve hafıza karmaşıklığını da azalttığı gözlemlenmiş ve bu gözlemler ışığında SERPENT şifresine yapılan diferansiyel-lineer atakların karmaşıklıkları azaltılarak bilinen en iyi ataklar hızlandırılmıştır. Makale Lightsec 2015 konferansında sunulmuştur (Tezcan 2015). Bu makale *07_Lightsec2015.pdf* dosya ismiyle yüklenmiştir.

2. **Truncated, Impossible, and Improbable Differential Analysis of ASCON**: Blok şifreleme algoritmaları birçok farklı çalışma modunda kullanılabilir ve genellikle güvenlik ve hız açılarından sayaç (counter) modu tavsiye edilir. Birçok özeliği olan bu modların eksiği ise kimlik denetimi (authentication) özelliğinin olmamasıdır. Bu nedenle

2014 yılında başlayan ve 2018 yılında sonuçlanması beklenen CAESAR yarışmasında kimlik denetimine sahip şifreleme algoritmaları yarışmaktadır. Projemiz boyunca yarışmaya katılan 55 algoritmanın proje konumuz olan değişim kutuları zafiyetleri incelenip raporlanmıştır. Bulduğumuz zafiyetler en iyi şekilde ASCON şifreleme algoritmasına uygulanabildiği için bu şifreye 5 döngülük tasarımcıların bulamadığı imkansız diferansiyeller bulunmuş ve 5 ve 6 döngülük ataklar verilmiştir. Uzmanlar tarafında elde edilen bu analiz sonuçları yarışmaya katılan algoritmaların güvenlik seviyelerini belirlemek için çok önemlidir. ASCON algoritması halen devam etmekte olan yarışmada ilk 15'e kalmıştır. ASCON için elde ettiğimiz sonuçlar ICISSP 2016 konferansında sunulmuştur (Tezcan 2016). Bu makale *08_ICISSP2016.pdf* dosya ismiyle yüklenmiştir.

3. **Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited**: Yeni kurulan ODTÜ Siber Güvenlik Bölümü'nde açılan CSEC 508 Applied Cryptology dersi dönem projesi olarak dersi alan öğrencilerden RECTANGLE ve PRIDE blok şifrelerine yapılmış diferansiyel atakların diferansiyel faktörler açısından doğruluklarının kontrol edilmesi ve kodların yazılarak doğrulanması istenmiştir. Çalışmalar sonucunda PRIDE şifresi için literatürde verilen 4 diferansiyel atağın da yanlış olduğu gösterilmiş, bu ataklar düzeltilmiş ve yeni elde edilen atakların zaman karmaşıklığının daha fazla olduğu gösterilmiştir. RECTANGLE şifresinin ilk hali için verilen diferansiyel atağın ise diferansiyel faktörler kullanılarak hızlandırılabileceği gösterilmiştir. Çalışma Lightsec 2016 konferansında sunulmuştur (Tezcan vd. 2016a). Bu makale *09_Lightsec2016.pdf* dosya ismiyle yüklenmiştir. Makaleler konferans sonrasında güncellenerek kitapta bölüm şeklinde basıldığı için, online olarak 8 Mart'ta yayınlanmıştır ver makalenin yer aldığı kitap 15 Nisan'da basılacaktır.

4. **On Differential Factors**: Bu çalışmada diferansiyel faktörlerin sonuçları bir araya getirilmiştir. Etkilenebilecek yeni üretilmiş blok şifrelerin listesi ve tahmini etkileri gösterilmiştir. Ayrıca bu çalışmada 8x8 ebatlarında değişim kutularına sahip blok şifrelerde de diferansiyel faktör olduğu gösterilmiştir. Dolayısıyla diferansiyel faktörlerin sadece hafif tasarım blok şifreleri değil, bütün blok şifreleri etkilediği gösterilmiştir. Bu çalışma ISCTURKEY 2016 konferansında sunulmuştur (Tezcan vd. 2016b). Bu makale *10_iscturkey2016..pdf* dosya ismiyle yüklenmiştir.

5. **Brute Force Cryptanalysis of Mifare Classic Cards on GPU**: Dünyada en çok kullanılan akıllı kartlardan biri olan Mifare Classic kartları CRYPTO1 şifreleme

algoritmasını kullanmaktadır. Bu kartların güvenlik açıkları literatürde çok iyi şekilde gösterilmiştir. Kartların temel versiyonuna yapılacak kaba kuvvet ataklarının GTX 280 ekran kartı kullanılarak 9 gün 8 saatte gizli anahtarı ele geçirebildiği bilinen bir sonuçtur. Bu çalışmada bitslice tekniği ve birçok başka optimizasyon tekniği kullanarak bu atağı GTX 970 ekran kartında 5 saatten kısa bir süreye düşürdük. Mifare Classic akıllı kartların gelişmiş sürümlerinde ise kaba kuvvet ataklarının GTX 460 ekran kartı kullanılarak 1 ayda ele geçirilebileceği bilinen bir sonuçtur. Kullandığımız optimizasyon teknikleri ile bu atağı GTX 970 ekran kartında 7 saatten kısa bir süreye düşürdük. Bu sonuçlar kısa anahtar kullanan şifrelerin ekran kartlarında çok hızlı bir şekilde kırılabileceğini göstermektedir. Sonuçlar ICISSP 2017 konferansında yayınlanmıştır (Tezcan 2017). Bu makale *11_ICISSP_2017.pdf* dosya ismiyle yüklenmiştir.

5.6 Sunumlar

Kabul alan ve sunulan makalelerin yanı sıra, proje süresince proje yürütücüsü ve araştırmacıları şu sunum ve seminer çalışmalarını gerçekleştirmiştir:

1. Doç. Dr. Ali Doğanaksoy, 31 Mayıs 2016 tarihinde Atılım Üniversitesi'nde düzenlenen Kimlik Denetimi ve Şifreleme Çalıştayı'nda konuşmacı olarak "Kriptografide Rastgelelik" başlıklı seminer vermiştir.
2. Dr. Cihangir Tezcan, 31 Mayıs 2016 tarihinde Atılım Üniversitesi'nde düzenlenen Kimlik Denetimi ve Şifreleme Çalıştayı'nda konuşmacı olarak "New Evaluation Criteria for S-boxes" başlıklı seminer vermiştir.
3. Dr. Cihangir Tezcan, 17 Şubat 2016 tarihinde Orta Doğu Teknik Üniversitesi Sürekli Eğitim Merkezi'nde "Kriptografi ve Siber Güvenlik" başlıklı bir seminer düzenlemiştir. 300'den fazla kişinin kayıt olduğu bu sunum sayesinde daha geniş kitlelere temel kriptografi bilgisi ve çalışmalarımız bazı sonuçları anlatılmıştır.

6 Sonuç

Bu çalışmada öncelikle sözde diferansiyel faktörler geliştirilmiştir. ASCON, PRESENT, SERPENT, PRIDE, RECTANGLE ve LBLOCK gibi şifrelere yapılan ataklar düzeltilmiş ve yeni ataklar elde edilmiştir. Elde ettiğimiz bu yeni analiz yöntemleri sayesinde mevcut şifrelerin kriptanalistler tarafından analizlerinin daha iyi yapılması mümkün olacaktır ve şifrelerin gerçek

güvenlik miktarları daha iyi anlaşılacaktır. Ayrıca bu yöntemler yeni şifreler tasarlanacağı zaman dikkate alınacağı için daha güvenli şifrelerin tasarlanması mümkün olacaktır.

Çalışmanın ikinci sonucuysa şifreleme algoritmalarının ekran kartları üzerindeki performanslarının elde edilmesidir. Algoritmaların yapılarına göre ekran kartlarının sıradan işlemcilerden 10-40 kat daha hızlı olduğu gözlemlenmiştir. Bu sayede teorik olarak elde edilen ve CPU kullanarak doğruluğunu kontrol etmenin yıllar süreceği atakların ekran kartları ile kısa sürede kontrol edilebileceği gösterilmiştir. Ayrıca AES, DES ve PRESENT için ekran kartlarında elde ettiğimiz optimize edilmiş kodlar, COPACOBANA ve RIVYERA gibi 120 FPGA'den oluşan makinelerden fiyat/performans olarak çok daha iyi sonuçlar vermiştir. Ekran kartları kullanılarak kriptografik zafiyetler içeren akıllı kart özellikli ODTÜ kimlik kartlarının birkaç saatte kopyalanabileceği gösterilmiş ve eski standart olan A5/1 şifresini kullanan GSM görüşmelerinin dinlenebileceği gösterilmiştir. Bu elde edilen hızlar sonucunda 80 bit ya da daha küçük anahtar kullanan kriptosistemlerin hiçbir güvenlik sağlamadığı gösterilmiştir.

6.1 Öneriler

Ekran kartlarının paralel gücü son 10 yılda bilimsel hesaplamalar için birçok bilim dalında kullanılarak daha önceden elde edilmesi zor olan sonuçlara ulaşılmıştır. Bu projede ekran kartları simetrik şifreleme algoritmaları olan ve yapısal olarak benzerlikler içeren blok şifreler ve akan şifreler için kullanılmıştır. Proje kapsamında alınan 3 ekran kartlı bilgisayar daha önceden elde etmemizin mümkün olmadığı sonuçları elde etmemizde çok büyük bir role sahiptir. Daha fazla işlem gücüne sahip olabilmek için ileride 8 ekran kartlı tek bir bilgisayar oluşturmayı hedeflemekteyiz. Bu şekilde oluşturulacak birkaç bilgisayarı da dağıtılmış sistem olarak kullanarak çok yüksek işlem gücüne sahip olmayı hedeflemekteyiz. Üniversitenin birçok bilim dalında kullanılabilecek bu tarzda oluşturulmuş bir laboratuvarın gerekliliği çok belirgindir ve hedefimiz ileride bu tarz bir laboratuvarı oluşturmaktır. Üniversitelerin kendi ekran kartı laboratuvarlarını kurması ve lisans düzeyinde paralel programlama derslerini vermesinin günümüzde bir zorunluluk haline geldiğini düşünmekteyiz.

Kriptografinin ekran kartlarından çokça faydalanabileceği diğer alanları ise bu proje konusu dışında olan açık anahtar kriptografisi ve kriptografik özet fonksiyonlarıdır. Bizim projemizle eş zamanlı olarak Hollanda'da araştırmalarını yürüten Marc Stevens 4 adet GTX 970 ekran kartı kullanan 16 tane masaüstü bilgisayar ile bir laboratuvar kurmuş ve bu toplam 64 ekran kartı ile aylar süren işlemler sonucunda 2^{57} SHA-1 özet fonksiyonu işlemi yaparak 8 Kasım 2015 tarihinde "Freestart Collision" elde etmiştir. Normalde özet fonksiyonları aynı başlangıç

vektörünü kullanır ama Freestart Collision'da atağı yapan kişi farklı başlangıç vektörleri kullanarak iki farklı mesajın aynı özet çıktısını vermesini sağlar. Bu sonuç direk olarak özet fonksiyonun güvenliğini kırmasa da özet fonksiyonun içyapısının kırılmasına neden olmaktadır. Marc Stevens bu başarısı sonucunda 2016 yılında yeni donanım almak ve araştırmalarına devam etmek için Google'dan 50.000$'lık ödül kazanmıştır. Ve daha sonra Google'ın GPU'larını da kullanarak 2^{65} SHA-1 işlemi yapmış ve bilinen ilk SHA-1 çakışmasını (collision) 23 Şubat 2017 tarihinde elde etmiştir. Bu sonuç SHA-1 kriptografik özet fonksiyonunun pratikte kırıldığını göstermektedir ve birçok kurum ve kuruluş bu duyurudan sonra SHA-1 algoritmasını kullanmayı bırakmıştır.

Veri tabanlarında birçok parolanın kendisi yerine parolanın kriptografik özet fonksiyonu çıktısı saklandığı için, ekran kartlarının özet fonksiyonları hızı birçok güvenlik konusunu etkileyecektir. Bu nedenle ekran kartlarının açık anahtar kriptografisi ve kriptografik özet fonksiyonları üzerindeki etkisinin akademik çalışmalar açısından yeni projelerde incelenmesi yeni kriptografik sonuçlar elde etmek ve güvenlik kriterlerini doğru belirlemek açısından son derece önemlidir.

NOT: *Projede araştırmacı olarak yer alan Dr. Cihangir Tezcan'ın TÜBİTAK 2219 desteği ile yurtdışı doktora sonrası çalışma yapması önceden planlanmıştır. Proje çalışmalarını aksatmamak için 15 Martta sonlanacak bu projemiz bittikten sonra 2 Nisan tarihinde yurtdışına çıkması planlanmıştır. Fakat proje 15 Mart'ta sonlanacak olmasına rağmen bu görev araştırmacının üzerinden ancak final raporu onaylandıktan sonra düşeceği ve dolayısıyla 2219 desteğini hemen başlatamayacağı bilgisi TÜBİTAK tarafından bildirilmiştir. Dolayısıyla Dr. Cihangir Tezcan TÜBİTAK 2219 desteğini başlatabilmek için proje bitimine 1 ay kala projeden ayrılmıştır ve bu durum proje çalışmalarında herhangi bir aksaklığa neden olmamıştır.*

7. Referanslar

1. Biham, E., Anderson, R.J., Knudsen, L.R. 1998. “Serpent: A new block cipher proposal”, FSE Lecture Notes in Computer Science, 1372, 222-238.
2. Biham E., Biyukov, A., Shamir A. 2005. “Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials”, Journal of Cryptology, 18(4), 291-311.
3. Biham, E., Shamir, A 1991. “Differential Cryptanalysis of DES-like Cryptosystems”, Journal of Cryptology, 4(1), 3-72.
4. Bilgin B., Nikova, S., Nikov, V., Rijmen, V., Stütz, G. 2012. “Threshold implementations of all 3x3 and 4x4 S-boxes”, CHES Lecture Notes in Computer Science, 7428, 76-91.
5. Blondeau, C. 2013. “Improbable differential from impossible differential: On the validity of the model”, INDOCRYPT Lecture Notes in Computer Science, 8250, 149-160.
6. Blondeau, C. 2013. “Improbable differential from impossible differential: On the validity of the model”, slides, http://users.ics.aalto.fi/blondeau/PDF/slide_indocrypt.pdf, Son erişim tarihi: 2 Kasım 2014.
7. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. 2007. “PRESENT: An ultra-lightweight block cipher”, CHES Lecture Notes in Computer Science, 4727, 450-466.
8. Browning, K. A., Dillon, J. F., McQuistan, M. T., Wolfe, A.J. 2010. An APN permutation in dimension six. In Finite Fields: Theory and Applications - FQ9, volume 518 of Contemporary Mathematics, pages 33–42. AMS.
9. Courtois, N., Pieprzyk, J. 2002. “Cryptanalysis of block ciphers with overdefined systems of equations”, ASIACRYPT Lecture Notes in Computer Science 2501, 267-287.
10. Dunkelman, O., Indesteege, S., Keller, N. 2008. “A differential-linear attack on 12-round Serpent”, INDOCRYPT Lecture Notes in Computer Science, 5365, 308-321.
11. Kocher, P.C., Jaffe, J., Jun, B. 1999. “Differential power analysis”, CRYPTO Lecture Notes in Computer Science, 1666, 388-397.
12. Knudsen, L.R. 1994. “Truncated and higher order differentials”, FSE Lecture Notes in Computer Science 1008, 196-211.
13. Langford, S.K., Hellman, M.E. 1994. “Differential-linear cryptanalysis”, CRYPTO Lecture Notes in Computer Science, 839, 17-25.
14. Matsui, M. 1994. “Linear cryptoanalysis method for DES cipher”, EUROCRYPT Lecture Notes in Computer Science, 765, 23-27.
15. Saarinen, M.J.O. 2011. “Cryptographic analysis of all 4x4 s-boxes”, SAC Lecture Notes in Computer Science, 7118, 118-133.

16. Tezcan C. 2010. “Improbable differential attack: Cryptanalysis of Reduced Round CLEFIA”, INDOCRYPT Lecture Notes in Computer Science, 6498, 197-209.
17. Tezcan, C. 2014. “Improbable Differential Attacks on PRESENT using Undisturbed Bits”, Journal of Computational and Applied Mathematics, 259, 203-511.
18. Tezcan, C., Özbudak, F. 2014. “Differential factors: Improved attacks on SERPENT”, Lightsec 2015, İstanbul, Turkey, Springer LNCS 8898, 69-84.
19. Tezcan, C., Temizel, A. 2014. “Cryptanalysis of PRESENT via CUDA devices”. GPU Technology Conference, poster 4192.
20. Tezcan, C. 2015. “Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT”, Lightsec 2015, Bochum, Germany, Springer LNCS 9542, 21-33.
21. Tezcan, C. 2016. “Truncated, Impossible, and Improbable Differential Analysis of ASCON”, Proceedings of ICISSP 2016, Rome, Italy, 325-332.
22. Tezcan, C., Okan, G. O., Şenol, A., Doğan, E., Yücebaş, F., Baykal N. 2016. “Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited”, Lightsec 2016, Aksaray, Turkey, Springer LNCS 10098, 18-32
23. Tezcan, C., Doğanaksoy, A., Okan, G. O., Şenol, A., Doğan, E., Yücebaş, F., Baykal N. 2016. “On Differential Factors”, ISCURKEY 2016, Ankara, Turkey, 103-110.
24. Tezcan, C. 2017. “Brute Force Cryptanalysis of Mifare Classic Cards on GPU”, Proceedings of ICISSP 2017, Porto, Portugal, 524-528.
25. Wang, M., 2008. Differential cryptanalysis of reduced-round PRESENT. In: Vaudenay, S. (ed.) AFRICACRYPT. Lecture Notes in Computer Science, vol. 5023, pp. 40-49. Springer