

Akış Şifrelerinde Tasarım Teknikleri ve Güç İncelemesi

M. Tolga Sakallı, Ercan Buluş, Andaç Şahin, Fatma Büyüksaraçoğlu

Bilgisayar Mühendisliği Bölümü Mühendislik Mimarlık Fakültesi Trakya Üniversitesi, 22030, Edirne
tolga@trakya.edu.tr, ercanb@trakya.edu.tr, andacs@trakya.edu.tr, fbyuksaracoglu@trakya.edu.tr

Özet: Simetrik şifreler bilgi güvenliğinin sağlanmasında önemli rol oynarlar. Bu şifreleri blok ve akış şifreler olmak üzere iki ana kategoriye ayırabiliriz. Buna ek olarak güvenli şifreler tasarlamak kriptolojinin en önemli konusudur. Son zamanlarda blok şifreler ile ilgili olarak güvenliğin daha iyi anlaşıldığı gözlenmektedir. Diğer yandan, akış şifreler eski popülerliğini kaybetmişlerdir. Bunun sonucu olarak 2004 yılında daha güçlü akış şifre geliştirmek ve akış şifrelere eski popüleritesini tekrar kazandırmak amacıyla eSTREAM projesi başlatılmıştır. Bu çalışmada yeni akış şifreleme tasarım teknikleri ve eSTREAM projesi kapsamında bu şifrelere karşı bazı önemli saldırı tipleri incelenmiştir. Buna ek olarak bu çalışma akademik camiada akış şifreler üzerine devam eden çalışmaların yönünü bulmaya amaçlamaktadır.

Anahtar Kelimeler: Akış Şifreler, Tasarım Teknikleri, Akış şifrelere karşı Saldırımlar

Abstract: Symmetric ciphers are very important for providing information security. These ciphers can be categorized into two groups which are block ciphers and stream ciphers. In addition, cryptology is related with designing secure ciphers. In the last few years, the security of block ciphers seems to better understood. On the other hand, stream ciphers have lost their old popularity. As a consequence, a project called eSTREAM which aims stronger stream ciphers to be developed and to regain stream ciphers' old popularity has been launched in 2004. In this study, we examine new stream ciphers' design techniques and some cryptanalytic attacks in view of eSTREAM project. In addition, we aim to find out the direction of outgoing researches on stream ciphers in academic community.

Keywords: Stream Ciphers, Design Techniques, Cryptographic Attacks against Stream Ciphers.

1. Giriş

Şifreleme yöntemleri ve bu yöntemlere karşı yapılan saldırılar sayısal verinin korunmasında ya da güvenli bir şekilde iletilmesinde kullanılan şifreleme algoritmalarının tasarımında ve bu algoritmaların güvenliklerinde önemli bir yer teşkil etmektedir. Şifreleme algoritmaları, bir anahtar yardımıyla, sayısal verinin anlaşılmasız hale dönüştürülmesi işlemi gerçekleştirirler. Bir şifreleme algoritması kullanılarak gerçekleştirilen şifreleme işlemi sonucunda elde edilen şifreli metin anahtar bilinmeden deşifre edilememelidir.

Şifreleme algoritmalarını temelde simetrik, asimetrik ve hash algoritmaları olmak üzere üç

gruba ayırabiliriz. Bunlardan simetrik şifreleme algoritmaları ise blok ve akış şifreleme algoritmaları olmak üzere iki gruba ayrılabilir. Blok şifreleme algoritmaları köklerini *Shannon*'un [1] ortaya koyduğu karıştırma ve yayılma tekniklerinden almaktadır ve sabit uzunluktaki veri bloklarını şifreleme işlemine tabi tutarlar. Karıştırma şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken, yayılma açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır. Blok şifrelerin tasarımında karıştırma ve yayılma, sırasıyla *yer değiştirme* ve *doğrusal dönüşüm* işlemleri ile gerçekleştirilir. Bu tip şifreleme algoritmalarında SPN (Substitution Permutation Networks) ve Feistel olmak üzere iki temel tasarım mimarisi

vardır ve blok şifreleme algoritmalarına örnek olarak AES (Advanced Encryption Standard) [2] verilebilir. İkinci kategoriye ait simetrik şifreleme algoritmaları olan akış şifreler ise açık metnin bir karakterine bir seferde zamanla değişen bir şifreleme fonksiyonu kullanarak açık metnin karakterlerini ayrı ayrı şifreler. 1949 da Shannon 'tek kullanımlık şeritlerin (one-time pad) anahtarın rastlantısal olma ve bir kereliğine kullanılma şartları ile koşulsuz güvenli olduğunu göstermesinden sonra bu şifrelerde en önemli kısıtlama olarak anahtar uzunluğunun mesaj uzunluğuna eşit olması gerekliliği olarak ortaya çıkmıştır. İşte akış şifreleri bir anahtarla üretici besleyerek mümkün olduğu kadar uzun periyotlu ve rastlantısal gözüken anahtar dizilerini üretmeyi amaç edinir ve elde ettiği anahtarları açık metinle şifreleme fonksiyonuna sokarak şifreli metni elde eder. Akış şifrelere örnek olarak RC4 [3] ve SEAL [4] verilebilir.

Diğer yandan kriptanaliz, kriptografik yapıların kırılmasında kullanılan tekniklerin çalışılması anlamına gelmektedir ve kısaca şifre kırma bilimidir. Bir şifrenin gücü değerlendirilirken genellikle geniş arama saldırısı (exhaustive key search) bir kıstas olarak karşımıza çıkmaktadır. Geniş anahtar arama saldırısı k bit anahtara sahip bir şifre için olası tüm anahtarların, 2^k , denendikten sonra anlamlı mesaj elde edilip edilmemesine göre anahtarları elde etme yöntemidir. Kriptografik yapıların kırılması niyetiyle geliştirilen saldırılarda saldırı yapılan kriptosistemin bilindiği kabul edilir (Kerckhoffs'un prensibi) ve buna ek olarak bir kriptosisteme saldırılabilmek için sahip olunması gereken veriler vardır. Bu sahip olunan verilere göre saldırı modellerinden biri seçilebilir. Bu saldırı modellerinden en yaygın olanları şunlardır: *Sadece şifreli metin saldırısı*; Düşman şifreli metin dizisine sahiptir, *Bilinen açık metin saldırısı*; Düşman açık metin dizisine ve

bunların şifreli metin dizisine sahiptir, *Seçilmiş açık metin saldırısı*; Düşman bir açık metin dizisini seçebilir ve bunların şifreli metinlerini oluşturabilir, *Seçilmiş şifreli metin saldırısı*; Düşman bir şifreli metin dizisi seçebilir ve bunların açık metinlerini oluşturabilir. Yukarıdaki saldırı modellerine bakıldığında modeller pratikte uygulanabilirliği kolay olandan zor olana doğru sıralanmıştır. Bu saldırı modellerinden en gerçekçi olan model sadece şifreli metin saldırısıdır. Diğer saldırı modelleri gerçekte bir şifrenin derecelendirilmesinde bir ölçüt teşkil etmektedir. Örneğin seçilmiş açık metin saldırısına karşı dayanıklı bir şifre dayanıklı olmayana göre daha güvenli olacaktır. Ek olarak pratikte mümkün olmayacak saldırı modellerinin kullanılması belki de güvenliği hiç bir zaman ispatlanamayacak bir şifreye bir güvenlik payı ekleyeceğini unutmamak gerekir. Ancak bunun yanında eğer bir şifre sadece şifreli metin saldırısına karşı "çok gerçekçi bir saldırı modeli" dayanıklı değil ise kesinlikle zayıf bir şifredir [5].

Bu çalışmada simetrik şifreleme algoritmalarının bir kategorisi olan ve şifreleme algoritmaları içindeki en hızlı algoritmalar olarak bilinen akış şifrelerinin güç incelemesi gerçekleştirilmiştir. Özellikle son yıllarda popüler olan bazı tasarım teknikleri ile saldırı yöntemlerine değiştirilmiş ve bu şifreleme algoritmalarının tasarım prensiplerinin gittiği yön belirlenmeye çalışılmıştır. Buna ek olarak blok şifreleme algoritmalarında oturmuş olan ancak akış şifrelerde belirli olmayan tasarım prensiplerinin sınıflandırılması da gerçekleştirilmiştir.

2. Akış Şifreler

Akış şifreler daha önceden de bahsedildiği gibi açık metnin bir karakterine bir seferde zamanla değişen bir fonksiyon uygulayarak açık metnin karakterlerini ayrı ayrı şifreler [6]. Akış şifreler eşzamanlı ve eşzamansız olmak üzere temelde ikiye ayrılırlar. Eşzamanlı akış şifrelerde anahtar dizisi, açık metin ve gizli anahtardan bağımsız olarak üretilir. Her iki şifreleme tipi de

1 Tek Kullanımlık Şerit: Mesaj bitleri

$M = m_1, m_2, \dots, m_s$ ve anahtar bitleri $K = k_1, k_2, \dots, k_s$

olmak üzere şifreli metin $c_i = m_i \oplus k_i, i = 1, \dots, s$ şeklinde gösterildiği gibi anahtar bitleri ile açık metin bitlerinin mod 2 toplamı yada XOR işlemi sonucu elde edilir.

sonlu durum otomatıdır ancak eşzamansız akış şifrelerde anahtar dizisi, sabit uzunluktaki bir önceki şifreli metinlerin ve anahtarın bir fonksiyonu ile elde edilir. Bu şifreleme algoritmalarından eşzamansız akış şifrelerde şifreleme v şifreli metin sembolüne bağlı olduğu için bir iletim hatası durumunda v sembol sonra şifrenin tekrar eş zamanlaması mümkün olacaktır. Böyle bir durum söz konusu olduğunda öteki v sembol hatalı olacaktır. Yani hata yayılması eşzamanlı şifrelere göre kötüdür. Ancak eş zamanlama düşünüldüğünde eşzamansız şifreler eşzamanlı olanlara göre daha iyidir. Eşzamanlı şifrelerde eş zamanlama tekrar sağlanamaz.

Temelde bakıldığında akış şifreler donanım ve yazılım uygulamaları için geliştirilmiş akış şifreler olmak üzere iki farklı kategoriye ayrılabilir. Donanım tabanlı geliştirilen akış şifrelerinin yapıtaşları olarak doğrusal geri beslemeli öteleyici saklayıcılar (Linear Feedback Shift Registers) gösterilebilir. Bunun nedeni olarak donanımsal uygulamalardaki uygunlukları, üretilen serinin geniş periyoda sahip olması ve iyi istatistiksel özellikler göstermesi verilebilir. Doğrusal geri beslemeli saklayıcılarda ki doğrusallığın yok edilmesi için boole fonksiyonları kullanılarak elde edilen Doğrusal Olmayan Birleşim Üreteçleri (Nonlinear Combination Generators) ve Doğrusal Olmayan Filtre Üreteçleri (Nonlinear Filter Generators) akış şifrelerinin iki farklı tasarım yöntemini temsil eder. Doğrusal Olmayan Birleşim Üreteçleri birden fazla doğrusal geri beslemeli öteleyici saklayıcının bir boole fonksiyonu ile birleşiminden meydana gelirken Doğrusal Olmayan Filtre Yaklaşımında bir tane doğrusal geri beslemeli saklayıcı kullanılır. Diğer yandan Doğrusal Olmayan Filtre Yaklaşımı, F_{2^n} genişletilmiş cismini kullanan ve yazılım yoluyla tasarlanan akış şifrelerinde tasarım için etkin bir yoldur. Bunun nedeni olarak F_{2^n} üzerine tanımlanan maksimum uzunluklu doğrusal geri beslemeli öteleyici saklayıcıları ötelenmesinin yazılımda oldukça maliyetli olması gösterilebilir [7]. Yine doğrusal geri beslemeli öteleyici saklayıcı temelli akış şifrelerin diğer bir kategorisi de saat kontrollü üreteçlerdir. Bu

tür şifrelerdeki tasarım felsefesinde saat vuruşlarının sayısını düzensiz sinyaller kullanarak kontrol etme fikri vardır. Saat besleme sinyali bir doğrusal geri beslemeli öteleyici saklayıcı olabileceği gibi şifrenin diğer içsel bir yapısı da olabilir. Bu metotla doğrusal geri beslemeli saklayıcıların çıkışında ki doğrusallığın yok edilmesi amaç edinilir.

Diğer tasarım mekanizmalarından biri de doğrusal olmayan durum kullanan mekanizmalardır. Bu mekanizmalardan RC4 rastlantısal olarak karıştırma temellidir. Bununla beraber doğrusal geri beslemeli saklayıcı temelli doğrusal olmayan güncellemeye sahip şifrelere örnek olarak E0 (Bluetooth da kullanılan akış şifre) [8] verilebilir. Bu tür şifrelerin tasarımında doğrusal geri beslemeli saklayıcının doğrusallığını yok etmek için doğrusal olmayan bir bellek eklenir. Doğrusal geri beslemeli saklayıcı tabanlı fakat doğrusal olmayan durum güncellemesine sahip olan diğer mekanizmalara örnek saat kontrollü üreteçler verilebilir. GSM de kullanılan A5 şifresi [9], alternatifli adım üretici ve ²eSTREAM adaylarından Decim [10], Mickey [11] ve POMARANCH [12] bu mekanizmalardandır. Bu tasarım mekanizmaları dışında doğrusal geri beslemeli saklayıcıların cebirsel saldırılar gibi saldırılar karşısında zayıf düşmesinin bir sonucu olarak kullanılan doğrusal olmayan geri beslemeli saklayıcıları (Nonlinear Feedback Shift Registers) kullanan şifreler de mevcuttur. Bu şifrelere örnek olarak eSTREAM adaylarından HC-256 [13] ve Trivium [14] verilebilir. Bu şifrelerden HC-256 yazılım tabanlı bir şifre iken Trivium donanım tabanlı bir şifredir. Yine doğrusal geri beslemeli saklayıcı türleri dışında blok şifreleri kullanan ya da blok şifre tasarım türüne sahip akış şifre türleri mevcuttur. Bu şifrelere örnek olarak eSTREAM adaylarından Phelix [15] ve LEX [16] verilebilir. Bu şifreleme algoritmalarından 2 eSTREAM: Akış şifreleri için ECRYPT'in yürüttüğü bir projedir. ECRYPT (European Network of Excellence for Cryptology) ise 2004 yılında başlatılan ve IST (Information Societies Technology) ile birlikte geliştirilmiş 4 yıl süre ile avrupadaki araştırmacıların bilgi güvenliği üzerine işbirliğini güçlendirmek için kurulmuş seçkin bir ağıdır.

LEX akış şifresi AES blok şifresini kullanmaktadır. Farklı bir tasarım örneği olarak Salsa20 [17] akış şifresi 64 byte girişe 64 byte çıkışa sahip bir hash fonksiyonudur.

Akış şifrelerin ayrıldığı diğer bir kategori de bu şifrelerin word tabanlı ya da bit tabanlı olup olmamaları ile ilgilidir. Yukarıdaki örnek verilen şifrelerden HC-256 word tabanlı iken Trivium bit tabanlı bir akış şifresidir.

3. Akış Şifreler için Önemli Kriptografik Özellikler ve Saldırı Teknikleri

Akış şifrelerinin önemli bir kısmında doğrusal geri beslemeli saklayıcılardan gelen doğrusallığı yok etmek için boole fonksiyon-ları kullanılmaktadır. Akış şifrelerinin gücü için önemli boole fonksiyonları ile ilgili bazı tanımlar aşağıda verilmiştir [18].

Tanım 1: Bir boole fonksiyonu $f, {}^3F_2^n$ den

F_2 ye bir harita olarak isimlendirilir. Kriptografide kullanıldığı şekil matematiksel yaklaşımdan biraz değişiklik göstermekle beraber bir boole fonksiyonunun kriptografide kullanıldığı şekliyle iki elemanı vardır: 0 ve 1. Bir boole fonksiyonu bir *doğruluk tablosu* (*truth table*) ile gösterilebilir. Doğruluk tablosu

$$f(x) = (f(\mathbf{0} \ . \ \mathbf{0} \) \ f(\mathbf{0} \ . \ \mathbf{1} \) \ , \dots \ , \ f(\mathbf{1} \ . \ \mathbf{1} \)$$

) şeklinde sıralanan f 'in fonksiyon değerlerini gösteren bir vektördür. Aynı şekilde

$$\hat{f}(x) = (-1)^f = 1 - 2f \text{ fonksiyonu } \{-1, 1\}$$

setine ait bir fonksiyon olmak üzere doğruluk tablosundaki vektörler $(-1)^f$ fonksiyon değerlerine karşılık geliyorsa bu tür gösterilime *kutup doğruluk tablosu* (*polarity truth table*) ismi verilir.

Tanım 2: F_2^n de bir f boole fonksiyonunu temsil etmenin diğer bir yolu da polinomsal bir gösterim tarzı olan cebirsel gösterim biçimidir (Algebraic Normal Form-ANF). (1) ifadesindeki gibi gösterilebilir.

$$\begin{aligned} f(x) &= f(x_1, x_2, \dots, x_n) = \sum_{u \in F_2^n} a_u \left(\prod_{i=1}^n x_i^{u_i} \right) \\ &= \sum_{u \in F_2^n} a_u x^u; \quad a_u \in F_2 \\ &= a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus a_2 x_1 x_2 \\ &\quad \oplus \dots \oplus a_{n-1} x_{n-1} x_n \oplus a_{123} x_1 x_2 x_3 \\ &\quad \oplus \dots \oplus a_{123\dots n} x_1 x_2 x_3 \dots x_n \end{aligned} \quad (1)$$

Tanım 3: Bir f boole fonksiyonunun cebirsel derecesi $\deg(f)$ yada kısaca d ile tanımlanır. f boole fonksiyonunun cebirsel derecesi

ANF formundaki $x_0^{a_0} \dots x_{n-1}^{a_{n-1}}$ terimlerinden değişken sayısı maksimum olan değerdir.

Tanım 4: Eğer bir f fonksiyonunun t giriş

bitinin kombinasyonu istatistiksel olarak bağımsız ise f fonksiyonuna t dereceden ilinti

(korelasyon) dayanıklı (correlation immunity)

denir ve $\mathcal{C}(t)$ olarak tanımlanır. Diğer bir de-

yişle $f \in \mathbf{b}_n$ olmak üzere giriş değişkenleri-

nin $x_{i_1}, \dots, x_{i_r}, i \leq r \leq t$ herhangi bir alt seti

sabitlenirse;

$\Pr(f(x) = 0 | (x_{i_1}, \dots, x_{i_r}))$
 $= \Pr(f(x) = 1 | (x_{i_1}, \dots, x_{i_r}))$ eşit-
 liğine sahip oluruz.

Tanım 5: İki boole fonksiyonunun, f, g den elde edilen boole fonksiyonunun doğruluk tablolarının ürünü $f.g$ (iki vektör arasında elde edilen nokta ürünü değil) ile temsil edilsin. F_2^n

üzerinde tanımlanmış bir boole fonksiyonunun cebirsel dayanıklılığı (algeb-raic immunity) (AI)

$$f.g = \bar{0} = (0,0,\dots,0) \text{ yada } (f \oplus \bar{1})g = \bar{0}$$

yapan F_2^n den F_2 ye tanımlı g fonksiyonunun en düşük derecesidir. $f.g = \bar{0} = (0,0,\dots,0)$ olacak şekilde fonksiyon g 'ye f 'in bir bozucusu (annihilator) denir. $An(f)$, f 'in tüm bozucularının setini tanımlar.

Tanım 6: Bir f boole fonksiyonunun doğrusal olmama özelliği en yakın affine fonksiyona olan hamming uzaklığı ile temsil edilebilir. \mathbf{b}_n , n değişkenli tüm boole fonksiyonların seti,
 $\Lambda_n = \{a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n; a_i \in F_2, 0 \leq i \leq n\}$

ise affine ($a_0 = 0$ ise doğrusal) yani 1. dereceden fonksiyonlar seti ve $d_H(f, a)$ iki fonksi-

yon arasındaki ⁵hamming uzaklığı olmak üzere $f \in \mathbf{b}_n$ boole fonksiyonunun doğrusal olma değeri (2) ifadesindeki gibi verilebilir.

$$N_f = \min_{a \in E_n} d_H(f, a)$$

$$= \min_{U_1, \dots, U_n, V \in \{0,1\}} \# \left\{ X | f(X) \neq \bigoplus_{i=1}^n U_i X_i \oplus V \right\} \quad (2)$$

Tanım 7: Bir Boole fonksiyonu $f : F_2^n \rightarrow F_2$ için doğruluk tablosundaki 0'ların sayısı 1'lerin sayısına eşitse boole fonksiyonu için dengeli denir. Dolayısıyla dengeli boole fonksiyonunun hamming ağırlığı 2^{n-1} dir.

Akış şifrelelere karşın değişen ve gelişmekte olan çeşitli saldırı teknikleri mevcuttur. Bu saldırı tiplerinden ilinti saldırıları (correlation attacks) doğrusal geri beslemeli öteleyici saklayıcının çıkışı ile anahtar dizisi arasında

$$P(u_i = s_i) \neq \frac{1}{2} \text{ olacak şekilde bir ilintinin ol-}$$

ması ile açıklanabilir (u_i doğrusal geri beslemeli öteleyici saklayıcının çıkışı ve s_i bilinen

anahtar dizisi sembolü). Hızlı ilinti saldırıları ise çıkış dizisinin, doğrusal geri beslemeli saklayıcının durumlarının bir takım doğrusal fonksiyonu ile ilişkili olmasını kullanır. Bu saldırılar daha çok doğrusal olmayan birleştirici ve filtre mekanizmalarına karşı mümkün olmaktadır ve doğrusal geri beslemeli saklayıcının geri besleme polinomunun seyrek olmaması ve

5 Hamming uzaklığı: f ve g olarak isimlendirilen iki boole fonksiyonu arasındaki hamming uzaklığı

$d_H(f, g) = (f(x) \oplus g(x))$ 'in doğruluk tablosunun hamming ağırlığı ya da doğruluk tablosundaki 1'lerin toplamı olarak ifade edilir.

birleştirici fonksiyonunun yüksek ilinti dayanıklılığına sahip olması ile engellenebilir. Ayrıca birleştirici fonksiyon olarak dengeli bir boole fonksiyonunun kullanım gerekliliği dengeli ve yüksek ilinti dayanıklı bir boole fonksiyonu kullanma gerekliliğini ortaya çıkarmaktadır.

Daha önceden de bahsedildiği gibi akış şifrelerin klasik yapısı birçok doğrusal geri beslemeli öteleyici saklayıcının bir boole fonksiyonu f ile birleştirilmesine dayanmaktadır. Cebirsel saldırılarda $(k_0, k_1, \dots, k_{n-1})$ doğrusal geri beslemeli öteleyici saklayıcının başlangıç durumu (initial state) ve çıkış $(s_i)_{i \geq 0}$ arasında doğrusal olmayan denklemler sistemi oluşturulur ve daha sonra bu sistem çözülür.

$$\left\{ \begin{array}{l} f(k_0, k_1, \dots, k_{n-1}) = s_0 \\ f(U(k_0, k_1, \dots, k_{n-1})) = s_1 \\ f(U^2(k_0, k_1, \dots, k_{n-1})) = s_2 \\ \vdots \\ \vdots \\ \vdots \end{array} \right. \quad (3)$$

(3) ifadesindeki denklemde U bağlantı fonksiyonunu ya da doğrusal güncelleştirici fonksiyonu, f filtre ya da birleştirici fonksiyonu tanımlamaktadır. $t \geq 1$ için U^t doğrusal bir fonksiyon olduğu için tüm eşitlikler f 'in derecesine eşittir. Bununla beraber Meier [19] takip eden 2 senaryo ile bu denklemlerin derecesinin azaltılabileceğini göstermiştir.

Senaryo 1: $(f \oplus \bar{1})h = \bar{0}$ olacak şekilde düşük dereceli ve sıfır olmayan bir h fonksiyonu vardır.

$$h(U^i(k_0, k_1, \dots, k_{n-1})) = 0, \forall i \text{ ve } s_i = 0$$

yada $(s_i \oplus 1)h(U^i(k_0, k_1, \dots, k_{n-1})) = 0$.

Senaryo 2: $f.g = 0$ olacak şekilde düşük dereceli ve sıfır olmayan bir g fonksiyonu vardır.

$$g(U^i(k_0, k_1, \dots, k_{n-1})) = 0, \forall i \text{ ve } s_i = 1$$

yada $s_i g(U^i(k_0, k_1, \dots, k_{n-1})) = 0$.

Courtois [20] tarafından ortaya konulan hızlı cebirsel saldırılar, cebirsel saldırılardan daha etkili olabilmektedir. Hızlı cebirsel saldırılarda saldırgan doğrusal geri beslemeli öteleyici saklayıcının başlangıç durumu ile çıkış fonksiyonunun bazı bitleri arasında birlikte ilişki kurarak sistemin derecesi d 'yi azaltmaya çalışır. Çünkü cebirsel saldırılar da görülmüştür ki cebirsel saldırıların karmaşıklığı anahtar genişliği ile poli-

nomsal, denklem sisteminin derecesi d ile üssel bir ilişkiye sahiptir. Eğer daha düşük dereceden yeni denklemler bulmak mümkün olursa toplam saldırı aşırı derecede hızlandırılabilir.

Yukarıdan anlaşılacağı gibi cebirsel derece ya da cebirsel dayanıklılık akış şifrelerinin tasarımında önemli bir yer almıştır. Diğer yandan bir boole fonksiyonunun cebirsel derecesi ile ilinti dayanıklılık derecesi arasında bir ödünleşim (tradeoff) vardır. f 'in cebirsel derecesi

$\deg(f) > 1$ olmak üzere n değişkenli bir boole

le fonksiyonunun ilinti dayanıklılığı

4. Sonuç

$n - 1 - \deg(f)$ geçemez [18]. Bundan dolaydır ki akış şifrelerin tasarımında yukarıda bahsedilen özellikler ışığında iki farklı yönde gelişme vardır. Bunlardan birincisi bahsedilen özellikleri doyuran çok değişkenli boole fonksiyonları arama, ikincisi tasarım stratejisini değiştirme. Bu tasarım stratejilerinden ilki birleştirici fonksiyonu sonlu bir durum otomatu ile değiştirmek (Bluetooth ta kullanılan E0 akış şifresinde olduğu gibi). İkincisi ise doğrusal geri beslemeli öteleyici saklayıcı yerine doğrusal olmayan öteleyici saklayıcı kullanmaktır. Bu tür akış şifrelere örnek olarak donanım uygulamaları için önerilmiş Trivium şifresi verilebilir. Trivium şifresinin sahte kodu aşağıda verilmiştir. Trivium şifresinin 288 bitlik başlangıç durumuna 80-bit anahtar ve 80-bit IV (initial value- başlangıç değeri) yüklenir ve durumun 286, 287 ve 288. bitleri hariç kalan diğer bitler 0 değerine çekilir [14]. Yükleme bittikten sonra durum (state) aşağıdaki sahte kodu verilen algoritma kullanılarak anahtar biti üretmeye hazır hale getirilir ve daha sonra aşağıda verildiği gibi bit bit değerler $N \leq 2^q$ olacak

şekilde üretilir.

Trivium şifresinin anahtar üreten sahte kodu:

for $i = 1$ to N do

$$t_1 \leftarrow u_6 + u_9$$

$$t_2 \leftarrow u_{162} + u_{177}$$

$$t_3 \leftarrow u_{243} + u_{288}$$

$$s_i \leftarrow t_1 + t_2 + t_3$$

$$t_1 \leftarrow t_1 + u_9 \cdot u_9 + u_{171}$$

$$t_2 \leftarrow t_2 + u_{175} \cdot u_{176} + u_{264}$$

$$t_3 \leftarrow t_3 + u_{286} \cdot u_{287} + u_0$$

$$(u_1 \cdot u_2, \dots, u_9) \leftarrow (t_3 \cdot u_1, \dots, u_2)$$

$$(u_9 \cdot u_9, \dots, u_{177}) \leftarrow (t_1 \cdot u_9, \dots, u_{176})$$

$$(u_{178} \cdot u_{179}, \dots, u_{288}) \leftarrow (t_2 \cdot u_{178}, \dots, u_{287})$$

end for

Blok şifre tasarım teknikleri günümüzde anlaşılır seviyeye gelmiştir. Bu tasarım tekniklerini kullanarak güçlü şifreleme algoritmaları tasarlanmıştır. Ancak aynı şeyi akış şifreler için söylemek mümkün değildir. Şu ana kadar kırılmamış akış şifresi yoktur. Yine de bu konudaki çalışmalar değerlendirilmesi devam edilen eSTREAM projesi kapsamında yarışan 34 şifre ile devam etmektedir. Özellikle blok şifrelerden çok daha hızlı olan güvenli akış şifreleri tasarlama kısıtlı kaynakların kullanıldığı güvenlik gerektiren uygulamalar için önemlidir.

Bununla beraber eSTREAM projesi kapsamında yarışan ve başarılı bir saldırı gözlenmeyen şifrelerden HC-256 ve Trivium doğrusal olmayan geri beslemeli öteleyici saklayıcıların akış şifrelerin tasarımında önemli bir noktaya geldiğinin de kanıtıdır. Diğer yandan şifrelerin istatistiksel olarak göstereceği başarım da bu şifrelerin gelecekte güvenlik uygulamalarında varolup olamayacaklarını gösterecektir.

Kaynaklar

[1] C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, No. 30, pp. 50-64, 1949.

[2] J. Daemen, V. Rijmen, *AES Proposal: Rijndael*, First Advanced Encryption Conference, California, 1998.

[3] B. Schneier, *Applied Cryptography - Protocols, Algorithms, and Source code in C*, John Wiley & Sons, Inc., 2nd edition, 1996.

[4] P. Rogaway and D. Coppersmith, *A software-optimized encryption algorithm*, In Ross Anderson, editor, **Fast Software Encryption**, pages 56-63. Springer-Verlag, 1994.

[5] V. Rijmen, *Cryptanalysis and Design of Iterated Block Ciphers*, PhD Thesis, October 1997.

- [6] A. Menezes, P. v. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
- [7] P. Ekdahl, On LFSR Based Stream Ciphers, PHd Thesis, November 2003.
- [8] Bluetooth S.I.G, *Specification of Bluetooth System*, v.1.2, 2003.
- [9] A. Biryukov, A. Shamir, and D. Wagner, *Real time cryptanalysis of A5/1 on a PC*, Fast Software Encryption FSE 2000 (B. Schneier, ed.), Lecture Notes in Computer Science, vol. 1978, Springer-Verlag, , pp. 1-18, 2000.
- [10] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin and H. Sibert, *The Stream Cipher DECIM*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [11] S. Babbage, M. Dodd, *The Stream Cipher MICKEY*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [12] C. Jansen and A. Kolosha, *The Stream Cipher POMARANCH*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [13] H. Wu, *The Stream Cipher HC-256*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>
- [14] C. De Cannière and B. Preneel, *The Stream Cipher Trivium*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [15] D. Whiting, B. Schneier, S. Lucks and F. Muller, *The Stream Cipher Phelix*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>
- [16] A. Biryukov, *The Stream Cipher LEX*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [17] D. J. Bernstein, *The Stream Cipher Salsa20*, eSTREAM, the ECRYPT Stream Project., 2005, available at: <http://www.ecrypt.eu.org/stream>.
- [18] M. T. SAKALLI, *Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi*, Phd Thesis, 2006.
- [19] W. Meier, E. Pasalic, and C. Carlet, *Algebraic attacks and decomposition of Boolean functions*, Eurocrypt 2004 (C. Cachin and J. Camenisch, eds.), Lecture Notes in Computer Science, vol. 3027, Springer-Verlag, pp. 474-491, 2004.
- [20] N. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, Crypto 2003 (D. Boneh, ed.), Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, pp. 176-194, 2003.