SETSCI Conference Indexing System,
Volume 3 (2018), 980-983

ISAS 2018-Winter
2nd International Symposium on Innovative Approaches in Scientific Studies
November 30 – December 2, 2018, Samsun, Turkey

TEA ve XTEA Şifreleme Algoritmaları İçin Kaos Tabanlı Kaydırma Dizisi Oluşturulması ve Uygulanması

Cebrail Çiflikli[1], Kadir Aba[2*+]

[1]Kayseri Vocational School, Erciyes University, Kayseri, Turkey
[2]Vocational School, Nevşehir Hacı Bektaş Veli University, Nevşehir, Turkey
[*]Corresponding author: aba@nevsehir.edu.tr
[+]Speaker: aba@nevsehir.edu.tr
Presentation/Paper Type: Oral/ Tam Metin

Özet – İlk olarak 1999 yılında RFID teknolojisinin kullanımının önerildiği bir sunumda kullanılan Nesnelerin İnterneti kavramı (IoT); cihazların kendi aralarında konuştuğu (veri iletişimi yaptığı, bilgi topladığı, toplanan bilgiler ile karar verdiği) bir ağ yapısı olarak adlandırılır. 1999 yılından günümüze gelinceye kadar milyonlarca cihaz internete bağlı hale gelmiştir. İnternete olan bağlılık aynı zamanda bu nesnelerin dış dünyaya açık olması anlamı taşımaktadır. Dış dünyadan herhangi bir kişi veya cihazın erişimine açık olan bu nesneler ister istemez masum olmayan kişi veya cihazlarında erişimine açık olacaktır. Bu cihazlarda gerekli güvenlik önlemleri alınmaz ise veya veriler şifrelenmez ise ciddi güvenlik açıkları doğar. Bu çalışmada kablosuz ağlarda da kullanılabilen TEA ve XTEA şifreleme algoritmaları için kodlama ve kod çözme aşamalarında kaos tabanlı yeni bir kaydırma dizisi önerilmiştir. Mevcut yapıda sabit olan kaydırma aşaması kriptanaliz işlemlerinde kolaylık sağlamaktadır. Bu çalışmada ise kaydırma işlemlerinin sabit yapısı yerine, başlangıçta belirlenen anahtara göre sözde rastgele bir kaydırma dizisi oluşturulması ve şifreleme ve şifre çözme işlemlerinde ise oluşturulan bu kaydırma dizisinin kullanılması önerilmiştir. Ayrıca güvenli blok şifreleme için gerekli olan karıştırma ve yayılma özellikleri de algoritmada mevcuttur. Bu sayede algoritma hızından çok fazla ödün vermeden TEA ve XTEA algoritmalarının güvenliği daha da artırılmıştır.

Keywords – *IoT, Kaos, Güvenlik, TEA, XTEA*

Abstract – Firstly, the concept of Internet of Things (IoT) used in a presentation in 1999, which suggested the use of RFID technology. IoT is called as a network structure where the devices talk to (data communication, collecting information and making decisions with the information collected) each other. Since 1999, millions of devices have been connected to the internet. The fact that the objects are connected to the internet means that the objects are open to the outside world. These objects may also be accessible to malicious persons. If the necessary safety precautions are not taken in these devices or the data is not encrypted, serious vulnerabilities arise. In this study, a new chaos based shift series has been proposed for coding and decoding steps for TEA and XTEA encryption algorithms. Shifting bits are fixed in the current structure. Therefore, cryptanalysis is easier to process. In this study, instead of the fixed structure of the shift process, it is proposed to create a chaos based pseudo-random shift series according to the key and the implementing in the encryption and decryption process. Also the confusion and diffusion features required for secure block encryption are available in the algorithm. In this way, the security of TEA and XTEA algorithms are further increased without compromising the algorithm speed.

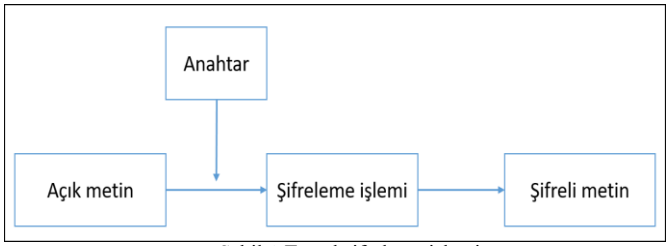
Keywords – *IoT, Chaos, Security, TEA, XTEA*

I. GİRİŞ

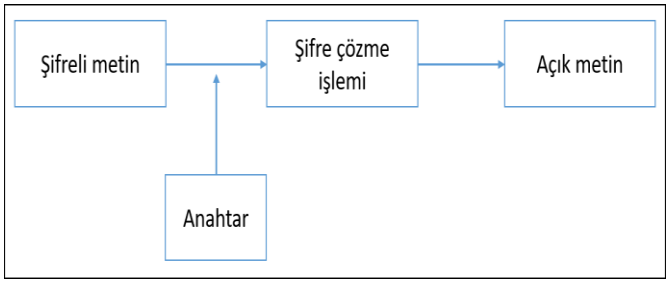
Nesnelerin İnterneti (IoT) kavramı, ilk olarak 1999 yılında RFID teknolojisinin kullanımının önerildiği bir sunumda kullanılmıştır [1]. Nesnelerin İnterneti kavramı, cihazların kendi aralarında veri iletişimi yaptığı, bilgi topladığı, toplanan bilgiler ile karar verdiği kısaca cihazların kendi aralarında konuştuğu bir ağ yapısı olarak adlandırılır [2]. Günümüzde birçok sistem bilgi güvenliği teknolojilerine ihtiyaç duyarlar. Nesnelerin interneti teknolojisinde de internete veya dış dünyaya bağımlılık vardır. Bu bağımlılık verilerin korunması ihtiyacını doğurur. Nesnelerin İnterneti kavramına temel oluşturan kablosuz algılayıcı ağlar, taşıdıkları verileri güvenli bir şekilde iletmek zorundalardır. Kablosuz algılayıcı ağların iletim kanalları ile algılayıcı düğümleri arasındaki iletişim saldırılara açıktır [4]. Literatürde, kablosuz algılayıcı ağlarda çeşitli güvenlik yapıları sunulmuştur. Veri şifreleme işlemi de sunulan güvenlik yapılarından birisidir. Veri şifreleme işlemi açık halde bulunan bir verinin bir anahtar yardımıyla anlaşılamaz hale dönüştürülmesi işlemidir. Şifreleme sonucu elde edilen şifreli metnin tekrar anlamlı hale dönüştürülmesi ise şifre çözme işlemidir.

Kaos doğrusal olmayan dinamik sistemlerde bulunan deterministik ve rasgele benzeri bir süreçtir. Kaotik sistemlerin önemli karakteristiklerinden biri sistem parametrelerine ve başlangıç koşullarına duyarlı olmasıdır. [3] Shannon, güvenli bir blok şifreleme için karıştırma ve yayılma özelliklerinin olması gerektiğini vurgulamıştır [5]. Sistem parametrelerinde meydana gelen küçük bir değişiklik sistem görüngelerinde büyük değişimlere sebep olmaktadır [6]. Kaosun bu yapısı karıştırma ve yayılma özelliklerini karşılamaktadır. [7,8] Bu çalışmada TEA ve XTEA algoritmaları için kodlama ve kod

çözme aşamalarında kaos tabanlı yeni bir kaydırma dizisi önerilmiştir. Önerilen yapı mevcut yapıya oranla algoritmaları kriptanaliz saldırılarına karşı daha dayanıklı hale getirmektedir. Kaotik sistemlere dayalı algoritmalar basit olduğundan dolayı [9] geliştirilen yeni kaydırma dizisi üretimi şifreleme algoritmalarının hızına olumsuz etkileri çok olmamaktadır.



Şekil 1 Temel şifreleme işlemi



Şekil 2 Temel şifrele çözme işlemi

II. Materyal Ve Metot

A. TEA (Tiny Encryption Algorithm)

TEA minimum hafıza alanı ve maksimum hız hedeflenerek oluşturulmuş bir şifreleme algoritmasıdır. Karışık cebirsel işlemleri kullanan ve Feistel türü bir şifreleme yapan bir algoritmadır [10]. Gömülü sistemlerdeki yüksek performansı, gerçekleme kolaylığı, hızlı olması, düşük enerji tüketimine imkan vermesi, düşük masraflı olması ve güvenli olması hafif (lightweight) olması özelliği ile TEA gömülü sistem tasarımlarına oldukça uygundur [11].

```
while (n-- > 0)
{
    sum += delta;
    y += (z << 4) + k[0] ^ z + sum ^ (z >> 5) + k[1];
    z += (y << 4) + k[2] ^ y + sum ^ (y >> 5) + k[3];
}
```

Şekil 3 TEA algoritması şifreleme kesiti

```
while (n-- > 0)
{
    z -= (y << 4) + k[2] ^ y + sum ^ (y >> 5) + k[3];
    y -= (z << 4) + k[0] ^ z + sum ^ (z >> 5) + k[1];
    sum -= delta;
}
```

Şekil 4 TEA algoritması şifre çözme kesiti

B. XTEA

XTEA algoritması, TEA algoritmasındaki zayıflıkları çözmek için geliştirilmiş bir blok kriptografik algoritmadır. XTEA tasarımcıları Cambridge Computer Lab'den David Wheeler ve Roger Needham'dır. XTEA algoritması, TEA algoritması gibi 128-bit anahtar uzunluğuna sahip bir 64-bit şifreleme algoritmasıdır.

```
while (n-- > 0)
{
    y += (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];
    sum += delta;
    z += (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3];
}
```

Şekil 5 XTEA algoritması şifreleme kesiti

```
while (n-- > 0)
{
    z -= (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3];
    sum -= delta;
    y -= (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];
}
```

Şekil 6 XTEA algoritması şifre çözme kesiti

C. Lojistik Harita

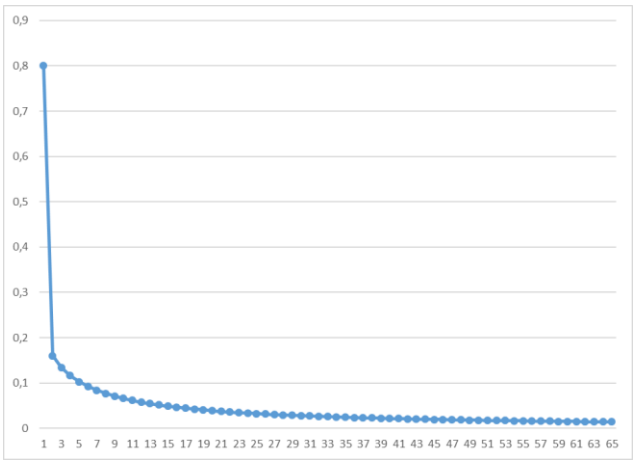
Koatik yapı, bir birine yakın iki başlangıç koşuluna farklı sonuçlar veren ve başlangıç koşullarına bağlı olan bir yapıdır. Kaosu düzensizlik ve karmaşıklığı belirlemek için kullanırız. Kaosu en iyi anlatan denklem ise lojistik haritalardır. Lojistik haritanın denklemi aşağıdaki gibi ifade edilir:

$$X_{n+1} = aX_n(1 - X_n) \quad (1)$$

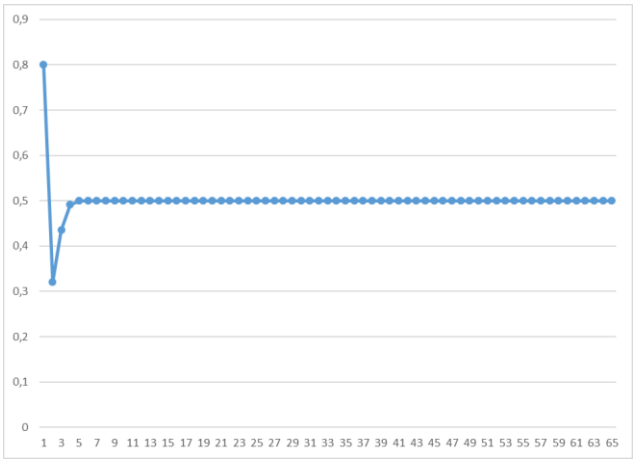
Denklemde $X \in [0,1]$ ve $a \in [0,4]$ olmak üzere göreceli olarak seçilebilirler. Denklemdeki n iterasyon sayısını göstermektedir. X_n ise n. kaotik sayıyı temsil etmektedir. Çalışmada başlangıç değeri olarak $X_0 = 0{,}8$ olarak belirlenmiştir. Başlangıç değeri belirlendikten sonra farklı a değerleri kullanılarak üretilen serilerde en iyi sonucu $a = 3{,}9$ değeri vermiştir. Farklı a değerleri kullanılarak üretilen serilerin şekil 7'de gösterilmiştir.

TEA ve XTEA algoritmalarını çalıştırmak için bir başlangıç anahtarına ihtiyaç vardır. Şifreleme anahtarı girildikten sonra bu anahtara bağlı olarak 0-8 arasında sözde rastgele 128 adet sayı üretilmiştir. Üretilen bu sayılardan kaotik serisine bağlı olarak 64 adeti alınmış ve kaydırma dizisi üretilmiştir. Bu 64 adet sayıdan oluşan kaydırma dizisi TEA ve XTEA algoritmalarının kodlama ve kod çözme aşamalarında kullanılmıştır. Üretilen kaotik sayı dizisinde yer alan sayıların virgülden sonraki ilk iki basamağı dikkate alınmış ve o sayılara rassal sayı dizisinde karşılık gelen sayılar seçilmiştir. Ve seçilen bu sayılar kodlama ve kod çözme aşamasındaki kaydırma işlemlerinde kullanılmıştır. Şekil 3,4,5 ve 6'da TEA ve XTEA algoritmalarının kodlama ve kod çözme aşamalarının bir kısmı yer almaktadır. Şekillerde de görüldüğü üzere aşamalarda kaydırma işlemleri için 4 ve 5 sayıları sabit olarak belirlenmiştir. Bu sabit yapıyı başlangıçta verilen anahtara göre sözde rastgele olarak belirlemek algoritmaların kriptanaliz işlemlerini zorlaştırmaktadır. Bu çalışmada ise sabit olarak belirlenen 4 ve 5 sayıları yerine kaotik diziden

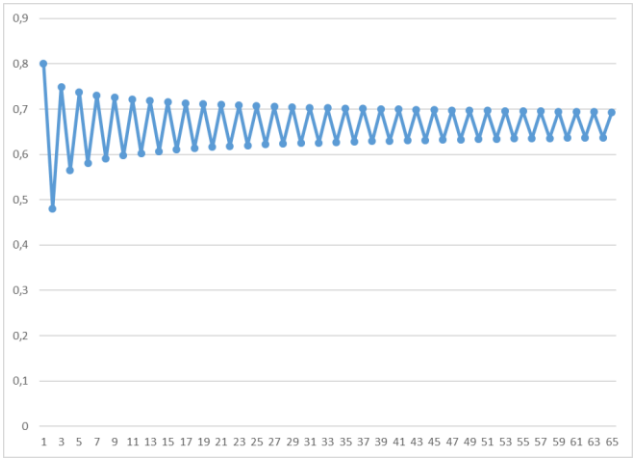
faydalanılarak üretilen ve 64 adet sayıdan meydana gelen kaydırma dizisi kullanılmıştır.



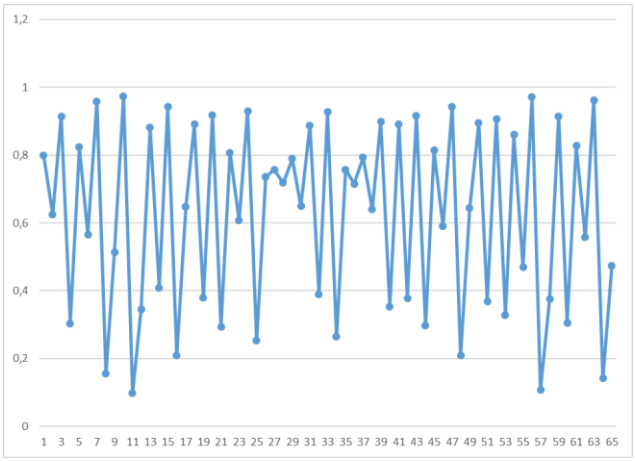
a



b



c



d

Şekil 7 Üretilen lojistik harita değerleri a) $a = 1$ b) $a = 2$ c) $a = 3$ d) $a = 3{,}9$

```
while (n-- > 0)
{
    sum += delta;
    y += (z << shift_array[Math.Abs(n-32)]) + k[0] ^ z +
        sum ^ (z >> shift_array[Math.Abs(n - 32)+1]) + k[1];
    z += (y << shift_array[Math.Abs(n - 32)]) + k[2] ^ y +
        sum ^ (y >> shift_array[Math.Abs(n - 32)+1]) + k[3];
}
```

Şekil 8 TEA algoritmasında önerilen kaydırma dizisinin şifreleme adımında kullanılması

TEA ve XTEA algoritmalarında değiştirebilir olmalarına rağmen 64 adet Fiestel turu yani 32 döngü tavsiye edilmektedir. Bu sebepten oluşturulan kaydırma dizisi 64 elemanlı olarak belirlenmiştir. Her bir döngüde ise önerilen kaydırma dizisinin 2 adet elemanı kullanılmaktadır.

Şifre çözme işlemlerinde şifreleme de olduğu gibi önerilen kaydırma dizisi kullanılmıştır. Kaydırma dizisi başlangıç parametreleri belli fakat anahtara bağlı olarak üretilen bir diziden türetildiği için şifreleme kullanılan dizinin aynısı şifre çözme işlemlerinde de üretilebilmektedir.

```
while (n-- > 0)
{
    z -= (y << shift_array[Math.Abs(n - 32)] ^ y >> shift_array[Math.Abs(n - 32)+1]) +
        y ^ sum + k[sum >> 11 & 3];
    sum -= delta;
    y -= (z << shift_array[Math.Abs(n - 32)] ^ z >> shift_array[Math.Abs(n - 32)+1]) + z ^ sum + k[sum & 3];
}
```

Şekil 9 TEA algoritmasında önerilen kaydırma dizisinin şifre çözme adımında kullanılması

III. BULGULAR

Önerilen kaydırma dizisi sözde rastgele olacak şekilde ve girilen şifreleme anahtarına bağlı olarak üretilmiştir. Ayrıca kaotik yapıdan faydalanılarak üretilen rassal sayılar kaotik sayılardan yardım alınarak seçilmiştir. Böylelikle algoritmaların kriptanaliz saldırılarına karşın güçlenmesi sağlanmıştır. Önerilen yöntem basit işlemler gerektirdiği için algoritmalar üzerine fazla işlem yükü düşürmemektedir. Algoritmalar daha güçlü hale gelmesine karşın sadece %5'lik bir zaman kaybı yaşanmıştır. Bu zaman kaybı da birçok ortamda önemsenmeyecek kadar düşüktür.

IV. TARTIŞMA VE SONUÇ

Bu çalışmada TEA ve XTEA algoritmaları için kaos tabanlı yeni bir kaydırma dizisi üretimi önerilmiştir. Kaos yapısından faydalanılarak üretilen bu aydırma dizisi sayesinde algoritmalar kriptanaliz saldırılarına karşı daha güçlü hale gelmiştir. Bunun yanında önemsenmeyecek kadar küçük bir zaman kaybına yol açmıştır.

Literatürde kaos tabanlı S-Box tasarım algoritmalarına bakıldığında kaos yapısı kullanılarak üretilen S-Box üretiminin yanına sıra satır ve sütun bazında döndürme ve karıştırma gibi evrelerin olduğu görülmektedir. Bu çalışmada da sadece kaos yapısı değil anahtara bağlı rastgele sayı üretme ve bu sayıların yine kaos yapısına bağlı bir şekilde seçilmesi ele alınmıştır.

İleriki çalışmalarda oluşturulan kaydırma dizisinin başka şifreleme algoritmalarına göre uyarlanması araştırılacaktır.

KAYNAKLAR

[1] Kutup, Nejat. "Nesnelerin İnterneti: 4H, Her Yerden, Herkesle, Her Zaman, Her Nesne İle Bağlantı." 16. Türkiye'de İnternet Konferansı inet-tr'11,2011.

[2] Aktaş, Faruk, Celal Çeken, and Yunus Emre Erdemli. "Biyomedikal uygulamaları için nesnelerin interneti tabanlı veri toplama ve analiz sistemi." Tıp Teknolojileri Ulusal Kongresi, 25-27,2014

[3] Jakimoski G, Kocarev L., "Chaos and cryptography: block encryption ciphers." IEEE Trans Circ Sys – I, 48(2): 163 -169,2001

[4] Xu, J.F., "A Defense System for Wireless Sensor Networks", The Journal of Wireless Networks of Posts and Telecommunications, 18(2), 119-122,2011

[5] S.E. Şeker., (2009), "TEA (Tiny Encryption Algorithm)" [Online] Available: http://bilgisayarkavramlari.sadievrenseker.com/2009/06/10/tea-tiny-encryption-algorithm/

[6] Özkaynak, F., Özer, A. B., & Yavuz, S. "Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması.", IV. Ağ ve Bilgi Güvenliği Sempozyumu, 108, 2011

[7] Amigo, J. M., Ljupco Kocarev, and Janus Szczepanski. "Theory and practice of chaotic cryptography." Physics Letters A 366.3, 211-216,2007

[8] Alvarez, Gonzalo, and Shujun Li. "Some basic cryptographic requirements for chaos-based cryptosystems." International journal of bifurcation and chaos 16.08, 2129-2151,2006

[9] Milani, Mir Mohammad Reza Alavı, Hüseyin Pehlivan, and Sahereh Hosein Pour. "Kaos tabanlı bir şifreleme yöntemi ve analizi." Akademik Bilisim, 487-493,2013

[10] A.Ç. Bağbaba, et al. "JPEG Image Encrryption via TEA Algorithm", Signal Processing and Communications Applications Conference (SIU), pp. 2090-2093,2015

[11] M.B. Abdelhalim, et a. , "Implementation of a Modified Lightweight Cryptpgraphic TEA Algorithm in RFID System", in 6th International Conference of Internet Technology and Secured Transactions., Abu Dhabi, United Arab Emirates, pp. 509-513,2011