Uluslararası Bilişim Sistemleri ve Uygulamaları Dergisi
International Journal of Information Systems and Applications

https://dergipark.org.tr/pub/ubsud

Araştırma Makalesi		Cilt No:	1	Sayı No:	1
Geliş Tarihi:	21.06.2025	Kabul Tarihi:	04.07.2025	Yayın Tarihi:	20.07.2025

VERNAM ŞİFRELEME VE PELL-LUCAS DİZİLERİYLE GÜÇLENDİRİLMİŞ SAYISAL İMZA TASARIMI

Tuğba GÖRESİM TOSKA[1] Ahmet KARAOĞLU[2] Emel SOYLU[3]

***Bu makale Tuğba GÖRESİM TOSKA tarafından hazırlanan "Sayılar Teorisine Dayalı Gelişmiş İmza Algoritmalarının Geliştirilmesi" başlıklı yüksek lisans tezinden türetilmiştir.**

Özet

Bugünün dijital dünyasında veri güvenliği sadece şifreleme ile değil, aynı zamanda verilerin bütünlüğünü vurgulayarak ve koruyarak mümkündür.Sayısal imza algoritmaları bu gerekliliği karşılamak için geliştirilmiş mekanizmalardır. Bu çalışma, Pell-Lucas dizisi kullanılarak güçlendirilen klasik Vernam şifrelemesine dayalı bir sayısal imza algoritmasıdır. Pell-Lucas dizisi, deterministik yapısı ve hızlı büyümesi sayesinde, rastgelelik gerektirmeden yüksek entropili anahtar üretimine olanak sağlamaktadır (Koshy, 2001; Vajda, 1989).Bu yöntemde açık anahtar dizisi, Pell-Lucas dizisinin modüler şekliyle XOR'lanarak özel anahtar elde edilmekte ve bu özel anahtar ile mesaj karakterleri tekrardan XOR işlemi yapılarak sayısal imza üretilmektedir. Doğrulama süreci, iletilen imza ve açık anahtar ile mesajın tutarlılığının test edilmesine dayanmaktadır. Lucas dizisi tabanlı benzer çalışmalardan farklı olarak (Duman & Duman, 2021), bu çalışma daha yüksek sayı alanı, lineer olmayan yapı ve doğrudan imza üretimi gibi özelliklerle literatüre yenilikçi bir katkı sunmaktadır.

Anahtar Kelimeler: Pell-Lucas dizileri, Vernam, Kriptoloji, İmza algoritmaları

VERNAM ENCRYPTION AND NUMBER SERIES OF PELL-LUCAS FOR A REINFORCED DIGITAL SIGNATURE DESIGN

Abstract

In today's digital world, data security is possible not only through encryption, but also by emphasizing and protecting the integrity of the data.. Digital signature algorithms are mechanisms developed to meet this requirement. This work is a digital signature algorithm based on the classical Vernam encryption strengthened using the Pell-Lucas sequence. Due to its deterministic structure and fast growth, the Pell-Lucas sequence enables high-entropy key generation without randomization (Koshy, 2001; Vajda, 1989). In this method, the public key sequence is XOR with the modular form of the Pell-Lucas sequence to obtain a private key and the message characters are XOR again with this private key to generate a digital signature.. The verification process is based on testing the consistency of the message with the transmitted signature and public key. Unlike similar works based on Lucas sequences (Duman & Duman, 2021), this work makes an innovative contribution to the literature with features such as higher number field, non-linear structure and direct signature generation.

Keywords: Pell-Lucas sequences, Vernam, Cryptology, Signature algorithms.

[1]Öğrenci, Samsun Üniversitesi, Yazılım Mühendisliği Bölümü, 230708004@samsun.edu.tr, https://orcid.org/0009-0005-5728-8564.

[2] Dr.Öğr.Üyesi, Sinop Üniversitesi, Bilgisayar Mühendisliği Bölümü, akaraoglu@sinop.edu.tr https://orcid.org/0000-0002-7507-3031.

[3] Dr.Öğr.Üyesi, Samsun Üniversitesi, Yazılım Mühendisliği Bölümü, emel.soylu@samsun.edu.tr, https://orcid.org/0000-0003-2774-9778.

1. GİRİŞ

Günümüzde dijital iletişim araçlarının yaygınlaşması ile veri güvenliğini hem bireysel hem de kurumsal düzeyde vazgeçilmez bir ihtiyaç hâline getirmiştir. Elektronik ortamda iletilen bilgilerin gizliliği, bütünlüğü ve doğruluğu; şifreleme tekniklerinin yanı sıra, gönderici kimliğini doğrulayan sayısal imza mekanizmalarıyla da sağlanmaktadır (Stinson, 2006). Bu nedenle geliştirilen şifreleme algoritmaları, hem bilgiye izinsiz erişimi engellemeyi hem de verinin göndericiye ait olduğunun doğrulanmasını amaçlamaktadır. Fakat artan siber tehditler, geleneksel olarak adlandırılan RSA, DSA ve AES gibi algoritmaların yeterliliğini sorgulatmakta ve daha hafif, uygulanabilir ve kuantum sonrası dirençli alternatiflere olan ihtiyacı artırmaktadır (Mollin, 2006; Chen et al., 2016).Simetrik anahtarlı şifreleme sistemlerinden biri olan Vernam şifreleme, teorik olarak "kırılamaz" kabul edilmesine rağmen, yalnızca anahtarın tamamen rastgele ve mesajla aynı uzunlukta olması durumunda bu güvenlik düzeyini sağlayabilmektedir. Bu koşullar, genellikle pratik uygulamalarda sağlanamadığından Vernam algoritmasının kullanımı sınırlı kalmaktadır. Bu çalışmada ele alınan problem, anahtar üretiminde rastgeleliğe dayanmadan, güvenliği artıran ve tekrarlanabilirliği olan bir yapı kurma ihtiyacıdır. Problemi çözmek amacıyla çalışmada, Pell-Lucas dizisi kullanılarak her mesaj karakterine özel, deterministik ama yüksek varyasyon sağlayan bir anahtar üretim yöntemi önerilmiştir. (Pell- Lucas dizisi : $Q_0 = 2, Q_1 = 2$ ve $n > 1$ olmak üzere $Q_n = 2Q_{n-1} + Q_{n-2}$ yineleme bağıntısı ile belirtilen $\{Q_n\}_{n\,\epsilon\,N}^{\infty}$ biçiminde tanımlanan tamsayı dizilerine Pell-Lucas sayı dizisi adı verilir. Bu sayı dizisi $n \epsilon N$ için $Q_n\}$ = $\{2, 2, 6, 14, 34, 82, 198, 478, \ldots\}$ şeklindedir. Bu dizi, Lucas ve Fibonacci gibi klasik sayı dizilerine oranla daha hızlı büyüyen yapısıyla, şifreleme alanını genişletmekte ve tahmin edilmesi zor bir yapı sunmaktadır. (Koshy, 2001; Vajda, 1989). Pell-Lucas dizisi ile açık anahtarın bit düzeyinde (XOR) işlenmesi ile oluşturulan özel anahtarlar kullanılarak, her karakter için farklılaştırılmış dijital imzalar üretilebilmektedir. Çalışmanın temel amacı, klasik Vernam algoritmasının zayıf yönlerini deterministik ve konum odaklı bir yapı ile aşarak, hafif sistemlerde kullanılabilecek, güvenli ve uygulanabilir bir sayısal imza algoritması sunmaktır. Bu amaç doğrultusunda, algoritmanın matematiksel modeli ortaya konulmuş, pseudocode gösterimi eklenmiş, örnek uygulama üzerinden işleyiş adım adım gösterilmiş ve doğrulama süreci teorik olarak analiz edilmiştir. (XOR işlemi: eğer karşılaştırılan iki kavram aynıysa sonuç 1 değilse sonuç 0 olarak döner. Örnek olarak: (1101 XOR 1011 = 1001))

2. YÖNTEM

Bu çalışmada, klasik Vernam şifreleme yönteminin güvenliğini ve uygulanabilirliğini artırmak için, deterministik yapıya sahip Pell-Lucas dizisi ile güçlendirilmiş bir dijital imza algoritması önerilmiştir. Yöntem, üç temel aşamadan oluşmaktadır: Anahtar üretimi ve güçlendirme, imza oluşturma ve imza doğrulama.

2.1.Anahtar Üretimi (Pell-Lucas Dizisi ile Güçlendirme)

İlk olarak kullanıcı tarafından belirlenen uzunluğu $n+1$ olan bir açık anahtar dizisi seçilir:

$$K = (k_0, k_1, k_2, \dots, k_n), \qquad k_i \epsilon \mathbb{Z}_{256}$$

Bu dizi, Pell-Lucas dizisi ile XOR'lanarak özel anahtar dizisi K' elde edilir. Pell-Lucas dizisi Eşitlik 1'deki özyinelemeli formülle tanımlanır:

$$PL_0 = 2,\ PL_1 = 2,\ PL_i = 2PL_{i-1} + PL_{i-2},\ i \geq 2 \quad (1)$$

Mod 256 işlemi ile dizinin elemanları sınırlı aralığa çekilerek kullanılır (Eşitlik 2)

$$K_i' = k_i \oplus (PL_i \mod 256),\ \forall i \in [0, n] \quad (2)$$

Bu işlem, klasik anahtarın deterministik olarak güçlendirilmesini sağlar ve anahtar tahminine karşı direnç kazandırır (Vajda, 1989; Koshy, 2001).

(Burada $\oplus$ işlemi XOR işlemidir.)

2.2.İmza Oluşturma

ASCII formatındaki mesaj dizisi:

$$M = (m_0, m_1, m_2, \dots, m_n), \qquad m_i \epsilon \mathbb{Z}_{256}$$

Her mesaj karakteri karşılık gelen özel anahtar bileşeni (mesajda var olan harflerin ASCII kod karşılığı binary sisteme çevirilecek) ile XOR'lanır:

$$S_i = m_i \oplus K_i', \quad \forall i \in [0, n] \quad (3)$$

Elde edilen $S = (S_0, S_1, S_2, \dots, S_n)$ dizisi mesajın sayısal imzasını oluşturur. Bu yapı, Vernam tarzı şifrelemenin simetrik mantığını taşır ancak anahtar üretiminde rastgelelik yerine kontrollü deterministik büyüme içerir. (Stakhov, 2006).

2.3.İmza Doğrulama

Doğrulama süreci, gönderilen imza, açık anahtar ve Pell-Lucas dizisi kullanılarak yürütülmüştür. Her karakter için aşağıdaki işlem uygulanmıştır: (açık anahtar K', imza S ve iletilen mesaj M)

$$\widehat{m}_i = S_i \oplus K_i' = S_i \oplus (k_i \oplus (PL_i \mod 256)) = m_i \quad (4)$$

Bu eşitliğin $\forall i$ için sağlanması imzanın geçerli olduğunu kanıtlar. Bu yöntem, mesaj bütünlüğünü doğrulamakla kalmaz, aynı zamanda gönderenin anahtarı bilip bilmediğini test ederek kimlik doğrulama sağlar (Stinson, 2006).

2.4. Uygulama ve Kodlama

Şekil 1'de gösterilen **GenerateDigitalSignature** algoritması, verilen bir mesaj ve gizli anahtar kullanılarak dijital imza üretimini amaçlamaktadır. Algoritma, öncelikle Pell-Lucas serisine dayalı bir sayı dizisi olan Q dizisini başlatır ve oluşturur. Q dizisi, ilk iki elemanı 2 olarak başlatıldıktan sonra, her bir sonraki eleman, kendinden önceki iki eleman kullanılarak;

Q[i] = 2 * Q[i-1] + Q[i-2] formülü ile hesaplanır. Bu dizi, anahtarı güçlendirmek amacıyla kullanılır. Güçlendirme aşamasında, her bir orijinal anahtar elemanı K[i], karşılık gelen Q[i] değerinin 256 ile modülü alınarak ve ardından XOR işlemi uygulanarak yeni bir anahtar dizisi K'[i] elde edilir. Daha sonra mesajın her bir elemanı, bu güçlendirilmiş anahtarın ilgili elemanıyla XOR işlemine tabi tutularak imza dizisi S[i] oluşturulur. Sonuç olarak, algoritma dijital imza olarak kullanılacak olan S dizisini oluşturur. Bu yapı sayesinde, hem mesajın hem de anahtarın karıştırıldığı ve dışarıdan müdahale edilmesi zor bir imza sistemi sağlanmış olur.

```
Algorithm: GenerateDigitalSignature
Input: Message M = [m₀, m₁, ..., mₙ], Key K = [k₀, k₁, ..., kₙ]
Output: Signature S = [s₀, s₁, ..., sₙ]

1. Initialize Q[0] ← 2, Q[1] ← 2
2. For i from 2 to n:
       Q[i] ← 2 * Q[i-1] + Q[i-2]        // Pell-Lucas recurrence
3. For i from 0 to n:
       K′[i] ← K[i] XOR (Q[i] mod 256)   // Key strengthening
4. For i from 0 to n:
       S[i] ← M[i] XOR K′[i]             // Signature generation
5. Return S
```

Şekil 1. Önerilen algoritmanın pseudocode gösterimi

Şekil 2'de verilen algoritma, dijital imza doğrulama işlemini gerçekleştirmek amacıyla tasarlanmıştır. Bu algoritma, orijinal mesaj M, gizli anahtar K ve gönderici tarafından üretilmiş dijital imza S olmak üzere üç girdi alır. İlk olarak, Pell-Lucas serisine dayalı Q dizisi Q[0] = 2 ve Q[1] = 2 şeklinde başlatılır. Ardından, tıpkı imza oluşturma algoritmasında olduğu gibi, Q[i] = 2 * Q[i-1] + Q[i-2] formülüyle Q dizisinin geri kalanı oluşturulur. Bu diziden elde edilen değerler, anahtar güçlendirme aşamasında kullanılır. Güçlendirme işleminde, her K[i] elemanı, karşılık gelen Q[i] mod 256 değeriyle XOR işlemine tabi tutularak yeni bir K'[i] dizisi elde edilir. Son aşamada, her bir imza öğesi S[i], güçlendirilmiş anahtar öğesi K'[i] ile XOR'lanarak M'[i] adlı doğrulanan mesaj öğesi hesaplanır. Elde edilen M' dizisi, iletilen orijinal mesaj M ile karşılaştırılır. Eğer diziler tamamen uyuşuyorsa imzanın geçerli olduğu kabul edilir. Bu şekilde, algoritma dijital imzanın doğruluğunu ve bütünlüğünü başarılı bir şekilde kontrol eder.

```
Algorithm: VerifyDigitalSignature
Input: Signature S, Original Message M, Public Key K
Output: Boolean (True if valid, False if not)

1. Initialize Q[0] ← 2, Q[1] ← 2
2. For i from 2 to n:
       Q[i] ← 2 * Q[i-1] + Q[i-2]        // Pell-Lucas recurrence
3. For i from 0 to n:
       K′[i] ← K[i] XOR (Q[i] mod 256)   // Key strengthening
4. For i from 0 to n:
       If M[i] ≠ (S[i] XOR K′[i]):
           Return False
5. Return True
```

Şekil 2. Önerilen algoritmanın doğrulama pseudocode gösterimi

Örnek uygulama

"VERİGÜVENLİĞİ" mesajı ve "ANAHTARDİZİSİ" anahtarı kullanılarak, Pell-Lucas dizisi tabanlı Vernam şifreleme yöntemiyle nasıl bir dijital imza oluşturulur ve doğrulama işlemi nasıl gerçekleştirilir?

Tablo 1'de harflerin decimal, binary, ASCII karakter karşılıkları verilmektedir.

Tablo1. Harlerin ASCII karşılığı

Karakter	A	…	Z	A	b…
ASCII(Decimal)	65	…	90	97	98
Binary	01000001	…	01011010	01100001	01100010
Karakter	0	…	9		
ASCII(Decimal)	48	…	57		
Binary	00110000	…	00111001		

1. Pell-Lucas Dizisi Hesaplama

İlk olarak Pell-Lucas dizisi Eşitlik 5'te verildiği gibi şu şekilde hesaplanır: (Eşitlik 1'den). Tablo 2'de Pell-Lucas dizisinin ilk 13 terimi verilmektedir.

$$PL_0 = 2,\ PL_1 = 2,\ PL_i = 2PL_{i-1} + PL_{i-2},\ i \geq 2 \tag{5}$$

Tablo2. Pell-Lucas dizisi ilk 13 terimi

n	0	1	2	3	4	5	6	7	8	9	10	11	12
PL_n	2	2	6	14	34	82	198	478	1154	2786	6726	16238	39202

Sonra Eşitlik 2'ye göre anahtar güçlendirme uygulanır. Tablo 3'te anahtar güçlendirme sonucu verilmektedir.

Tablo3. Her bir harf için anahtar güçlendirme

i	Anahtar	K (ASCII)	PL_n	$K_i' = k_i \oplus PL_i$
0	A	65	2	67
1	N	78	2	76
2	A	65	6	71
3	H	72	14	70
4	T	84	34	118
5	A	65	82	19
6	R	82	198	148
7	D	68	478	414
8	İ	304	1154	850
9	Z	90	2786	2700
10	İ	304	6726	7022
11	S	83	16238	16189
12	İ	304	39202	39474

Üçüncü adımda Eşitlik 3'e göre şifreleme yapılmaktadır. Tablo 4 'te VERİGÜVENLİĞİ" mesajındaki her bir har için şifreleme sonuçları verilmektedir.

Tablo4. Her bir harf için şifreleme

i	Mesaj Karakteri	M (ASCII)	K' (Güçlendirilmiş)	$S_i = m_i \oplus K_i'$
0	V	86	67	21
1	E	69	76	9
2	R	82	71	21
3	İ	304	70	366
4	G	71	118	49
5	Ü	220	19	203
6	V	86	148	202
7	E	69	414	347
8	N	78	850	924
9	L	76	2700	2776
10	İ	304	7022	6726
11	Ğ	286	16189	15903
12	İ	304	39474	39178

Son olarak Eşitlik 4'e göre yapılan doğrulama adımına göre Tablo 5'te her bir harf için doğrulama sonucu verilmektedir.

Tablo5. Her bir harf için doğrulama

i	Şifreli	K (ASCII)	PL_n	K'	$\widehat{m}_i = S_i \oplus K_i'$	Mesaj Karakteri
0	21	65	2	67	86	V
1	9	78	2	76	69	E
2	21	65	6	71	82	R
3	366	72	14	70	304	İ
4	49	84	34	118	71	G
5	203	65	82	19	220	Ü
6	202	82	198	148	86	V
7	347	68	478	414	69	E
8	924	304	1154	850	78	N
9	2776	90	2786	2700	76	L
10	6726	304	6726	7022	304	İ
11	15903	83	16238	16189	286	Ğ
12	39178	304	39202	39474	304	İ

Şifreleme ve doğrulama adımlarından sonra sonuç olarak orjinal "VERİGÜVENLİĞİ" mesajının doğru şekilde çözüldüğü görülmektedir.

Ek olarak algoritmanın temelinde kullanılan XOR işlemi, 0–255 aralığında çalışan ASCII karakter setiyle uyumludur. Fakat Pell-Lucas dizisinin hızlı büyüyen yapısından dolayı $PL_i > 255$ olabilir. Bu durum güçlendirme işlemi sırasında aşağıdaki iki şekilde yönetilmiştir:

Mod 256 Uygulaması: Pell-Lucas dizisinin her terimi için Eşitlik 6'daki;

$$PL_i \bmod 256 \tag{6}$$

işlemi uygulanarak tüm değerlerin 0–255 aralığında kalması sağlanmıştır. Bu sayede XOR işlemi sonucu her durumda geçerli bir ASCII karşılığı olacak şekilde sınırlanmıştır.

ASCII Karakter Dönüşümünün Yalnızca Görsel Amaçlı Kullanılması: Şifreli çıktılar doğrudan karakter olarak değil, genellikle sayı (ASCII kod) dizisi olarak saklanır ve o şekilde iletilir. Bu, ASCII dışı veya kontrol karakteri üretme ihtimalinde verinin bozulmasını engeller. Alıcı taraf, bu sayısal imzayı tekrardan orijinal mesajla karşılaştırarak doğrulama yapar. Bu nedenle, şifreli karakterin yazdırılabilir olup olmaması algoritmanın güvenliğini etkilemez. Dolayısıyla, önerilen yapıda ASCII dışı değer üretme durumu teknik olarak mümkün olsa bile, bu durum algoritmanın doğruluğunu veya güvenliğini olumsuz etkilemez. Tüm işlemler sayısal bir biçimde yürütüldüğünden**,** ASCII dışı karakterlerin oluşturduğu görsel bozukluklar uygulama açısından pratik bir sorun oluşturmamaktadır.Aynı zamanda, ASCII karakter seti dışına çıkılması istenmeyen durumlarda, dizinin

modül değeri 128 gibi daha düşük bir sayıya sabitlenebilir veya çıktıların base64 gibi metne çevrilebilen formatlarda kodlanması önerilebilir.

3.LİTERATÜRLE İLİŞKİLENDİRME VE POST-KUANTUM PERSPEKTİFİ

Bu çalışmada önerilen Pell-Lucas tabanlı dijital imza yöntemi, klasik Vernam şifreleme sistemini deterministik bir sayı dizisi ile bütünleştirerek güvenliği artırmayı amaçlamıştır. Bu yaklaşım, anahtar üretiminde rastgeleliğe olan bağımlılığı azaltırken, şifreleme sistemine yapısal çeşitlilik kazandırmaktadır. Literatürde benzer amaçlarla farklı sayı dizilerinin kullanıldığı çalışmalar vardır. Örneğin, Lucas dizisi ile karakter eşleştirerek kriptolama öneren Duman ve Duman (2021), sayı dizilerinin kriptografik olarak kullanılabilirliğini göstermiştir. Benzer şekilde Fibonacci dizisi ve Q-matrisi temelli kriptografik yapılar da önerilmiş ve bu tür deterministik dizilerin özellikle hafif sistemlerde tercih edilebileceği vurgulanmıştır (Prajapat et al., 2012; Stakhov, 2006).

Diğer yandan, son yıllarda kuantum bilgisayarlara karşı dayanıklı (post-quantum) kriptografi yaklaşımları önem kazanmıştır. Yaygın kullanılan RSA, DSA gibi algoritmalar kuantum algoritmaları (özellikle Shor algoritması) karşısında kırılabilirken, simetrik yapıların (ör. hash tabanlı imzalar, kod tabanlı sistemler, lattice tabanlı kriptografi) bu tehditlere daha dayanıklı olduğu gösterilmiştir (Chen et al., 2016; Bernstein et al., 2009).Bu yüzden, önerilen Pell-Lucas tabanlı yapı, kuantum dirençli olmaya aday simetrik sistemler sınıfında değerlendirilebilir. Çünkü algoritmanın temelinde karmaşık matematiksel fonksiyonlar değil, hafif, hızlı ve doğrusal olmayan dizilerle güçlendirilmiş XOR işlemleri bulunmaktadır. NIST tarafından önerilen post-kuantum standartlara (örn. CRYSTALS-DILITHIUM, SPHINCS+) tam anlamıyla alternatif olmasa bile, özellikle kaynak kısıtlı sistemler için kuantum sonrası dönemde kullanılabilecek pratik çözümler arasında yer alma potansiyeline sahiptir (NIST, 2023). Bu sebeple önerilen algoritmanın hem geleneksel hem de kuantum sonrası güvenlik bağlamında daha geniş kapsamlı olarak değerlendirilmesi, bu alandaki literatüre katkı sağlayacaktır.

4. TEORİK GÜVENLİK ANALİZİ

Oluşturulan Pell-Lucas tabanlı sayısal imza algoritması, klasik Vernam şifreleme mantığını deterministik fakat lineer olmayan bir yapı ile bütünleştirip saldırılara karşı direnç kazanmayı hedeflemektedir. Bu bölümde, önerilen algoritmanın temel kriptanaliz çeşitlerine karşı teorik güvenliği değerlendirilmiştir.

4.1. Brute-Force (Kaba Kuvvet) Saldırıları

Brute-force saldırıları, bütün olası anahtar kombinasyonlarının sistematik olarak denenmesini esas alır. Önerilen algoritmada her karakter için güçlendirilmiş özel

anahtar kullanıldığından, saldırganın sadece düz ASCII karakterleri değil aynı zamanda Pell-Lucas dizisinin modüler biçimiyle XOR'lanmış değerlerini de çözmesi gerekir. Anahtar dizisi deterministik olsa da, her seferinde farklı bir Pell-Lucas terimi ile XOR işlemi yapılması nedeniyle anahtar uzayı doğrusal olarak değil, üstel olarak genişlemektedir. Bu yapı, klasik sabit anahtarlı Vernam uygulamalarına oranla kaba kuvvet saldırılarında başarılı olma ihtimalini önemli ölçüde azaltmaktadır.

4.2. Frekans Analizi

Klasik şifreleme yöntemlerinde sabit anahtarlar kullanıldığında, karakterlerin şifreli hâlleri tekrarlayan desenler oluşturabilir. Buda frekans analizi saldırılarına zemin hazırlar. Fakat önerilen algoritmada her bir karakter için farklı bir Pell-Lucas değeri ile işlenmiş bir anahtar kullanıldığından, aynı harf bile farklı pozisyonlarda farklı şifreli değerlerle temsil edilmektedir. Bu durum kriptogramda istatistiksel tutarlılığı bozar ve frekans temelli analizlerin geçersiz kalmasına sebep olur.

4.3. Bilinen Düz Metin (Known Plaintext) ve Seçilmiş Düz Metin (Chosen Plaintext) Saldırıları

Bu tür saldırılarda amaç, bazı düz metin-şifreli metin çiftlerini baz alarak anahtarı tahmin etmektir. Fakat önerilen yapı gereği, bir karakterin şifreli çıktısı sadece düz metin karakterine değil, aynı zamanda o pozisyona özel Pell-Lucas terimine ve açık anahtar karakterine bağlıdır. Bu yüzden, örneğin aynı düz metin ve aynı açık anahtar kullanılsa bile, Pell-Lucas dizisinin indeks bağımlılığı sebebiyle farklı karakter pozisyonlarında farklı XOR sonuçları oluşur. Böylelikle saldırganın bu ilişkiyi geri çözümlemesi yüksek düzeyde karmaşıklık içerir.

4.4. Doğrusal Kriptanaliz

Doğrusal kriptanaliz, şifreleme işlemini temsil eden doğrusal denklemleri çözerek anahtarları tahmin etmeye çalışır. Önerilen algoritma, XOR gibi doğrusal bir işlem kullansa bile, anahtar bileşenlerinin her birinin farklı ve zamanla değişen deterministik bir diziyle (Pell-Lucas) üretilmiş olması doğrusal çözüm üretimini zorlaştırır. Özellikle, algoritmanın her karakter pozisyonuna ait işlem yapması, doğrusal ilişki kurmaya yönelik genel ifadelerin oluşturulmasını zorlaştırmaktadır.

Sonuç olarak önerilen Pell-Lucas tabanlı imza algoritması, klasik saldırı türlerine karşı teorik olarak güçlü bir direnç göstermektedir. Anahtar üretiminde kullanılan dizinin hızlı büyüyen yapısı, konum duyarlılığı ve karakter çeşitliliği, hem istatistiksel analizlere hem de doğrusal tahmin yöntemlerine karşı önemli bir koruma sağlamaktadır. Gelecekte, algoritmanın bu savunma düzeylerinin deneysel olarak da test edilmesi önerilmektedir.

5. SONUÇLAR ve TARTIŞMA

Bu çalışmada, klasik Vernam şifreleme yönteminin, deterministik ve hızlı büyüyen bir sayı dizisi olan Pell-Lucas dizisi ile entegrasyonu sağlanarak yeni bir sayısal imza algoritması önerilmiştir.Literatürde sıklıkla kullanılan rastgele anahtarlara dayalı simetrik şifreleme yöntemlerinin bazı zayıf yönleri, oluşturulan bu algoritma ile konum tabanlı anahtar güçlendirme yoluyla giderilmeye çalışılmıştır. Özellikle her bir mesaj karakteri için farklı bir Pell-Lucas terimi ile işlem yapılması, bu algoritmaya pozisyon duyarlılığı kazandırmakta; bu da doğrusal saldırılara karşı ek güvenlik sağlamaktadır.

Kriptografik güvenlik analizi şunu göstermektedir; önerilen yapı kaba kuvvet saldırılarına karşı genişletilmiş anahtar uzayı sayesinde yüksek direnç sunmaktadır. Her bir karakter için farklılaştırılmış XOR işlemi uygulanması, şifreli çıktının istatistiksel yapısını bozarak frekans analizi gibi klasik kriptanaliz tekniklerini geçersiz kılmaktadır (Stinson, 2006).Ayrıca , bilinen veya seçilmiş düz metin saldırılarına karşı da, pozisyon bazlı değişken anahtar yapısı sayesinde, doğrudan eşleştirmeyi imkânsız hâle getirmektedir. Bu da, literatürde önerilen Lucas dizisi tabanlı yaklaşımlardan daha yüksek çeşitlilik ve entropi sunmaktadır (Duman & Duman, 2021). Önerilen algoritmanın dikkat çeken yönlerinden biri de, hafif sistemlerde çalışabilecek kadar düşük işlem maliyetine sahip olmasıdır. XOR işlemlerinin donanımda hızlı gerçekleştirilebilmesiyle bu yapı, özellikle IoT cihazları, gömülü sistemler ve mobil uygulamalar gibi kaynak kısıtlı ortamlarda dijital imza çözümü olarak değerlendirilebilir (Mollin, 2006). Buna ek olarak, algoritmanın yapısı gereği ASCII sınırlarını aşan değerler oluşturma riski, mod 256 işlemi ile kontrol altına alınmış ve sayısal doğrulama çıktıları görsel bozulmalardan bağımsız şekilde güvenli olarak elde edilmiştir. Bu yapı, yalnızca yazdırılabilir karakterlerle değil, doğrudan sayısal ASCII tabanlı imza üretimi gerektiren sistemlerde de uygulanabilirlik sağlamaktadır. Uygulama adımları net bir biçimde sunulmuş; algoritma pseudocode formatında tekrarlanabilir hâle getirilmiştir.

Son olarak, önerilen yapı henüz tam anlamıyla bir post-kuantum algoritma olmasa bile, simetrik ve deterministik yapısı itibarıyla kuantum bilgisayarların oluşturduğu potansiyel tehditlere karşı alternatif bir yaklaşım sunmaktadır (Chen et al., 2016; Bernstein et al., 2009). Geleneksel (konvansiyonel) algoritmaların kuantum algoritmalarıyla kırılabilir olduğu ortamda, XOR ve pozisyon tabanlı yapıların entropi üretme kapasitesi oldukça önem kazanmaktadır. Bu nedenle önerilen model, NIST'in post-kuantum kriptografi standartlarına doğrudan rakip olmasa da, özellikle hafif sistemler için post-kuantum dirençli yaklaşımlarla birlikte kullanılabilecek destekleyici bir imza mekanizması olarak değerlendirilebilir (NIST, 2023).

6. ÖNERİLER

Bu çalışmada oluşturulan Pell-Lucas dizisi tabanlı dijital imza algoritması, klasik Vernam yapısının deterministik dizilerle harmanlanarak nasıl güçlendirilebileceğini göstermiştir. Elde edilen bulgular neticesinde, algoritmanın hem kuramsal çerçevesinin geliştirilmesi hem de uygulama çeşitliliğinin artırılması amacıyla aşağıdaki öneriler sunulmaktadır:

Unicode Uyumlu Genişletme: Algoritma yalnızca ASCII karakter seti ile sınırlıdır. Fakat çok dilli ve küresel sistemlerin ihtiyacını karşılayabilmek adına algoritmanın Unicode karakter kümesiyle de uyumlu hâle getirilmesi gerekmektedir. Bu sayede farklı alfabelere sahip metinlerin imzalanması ve doğrulanması sağlanabilecektir. (Mollin, 2006).

Zaman Damgalı İmza Geliştirmesi: Sayısal imzalarda mesajın ne zaman oluşturulduğu kritik bir güvenlik unsurudur. Pell-Lucas dizisinin indekslerinin zamana bağlı olarak yeniden hesaplanması ile, algoritmanın zaman damgası içeren versiyonu oluşturulabilir. Bu ise doğrulama sürecinde zaman bazlı kontrol mekanizması sağlayacaktır (Stinson, 2006).

Donanım Tabanlı Gerçekleme ve Performans Testleri: Önerilen algoritma, düşük işlem maliyeti neticesinde özellikle IoT ve gömülü sistemlerde uygulanmaya elverişlidir. Bu nedenle, donanım düzeyinde (ör. FPGA, mikrodenetleyici) gerçek zamanlı prototipler üretilerek, işlem süresi, bellek tüketimi ve enerji verimliliği gibi metrikler üzerinde performans analizi yapılması önerilmektedir.

Post-Kuantum Güvenlik Açısından Değerlendirme: Algoritmanın yapısı, kuantum öncesi klasik saldırılara karşı güçlü olsa bile, kuantum kriptanaliz perspektifinden henüz ayrıntılı olarak test edilmemiştir. Özellikle, Grover veya Shor algoritmalarına karşı direnç düzeyinin teorik olarak analiz edilmesi ve gerektiğinde Pell-Lucas dizisinin karmaşıklığının artırılması önerilmektedir (Chen et al., 2016; Bernstein et al., 2009).

Modüler Alan ve Blok Tabanlı Yaklaşım Geliştirme: Pell-Lucas dizisinin hızlı büyüyen yapısı, ASCII karakter alanını aşabilen sonuçlar oluşturabilir. Bu durumu kontrol edebilmek amacıyla farklı modüler alanlarda (örneğin mod 128, mod 512) algoritmanın uygulanabilirliği test edilebilir. Ayrıca, karakter bazlı yerine sabit boyutlu veri bloklarıyla çalışan bir versiyon geliştirilerek, algoritmanın büyük veriler üzerindeki verimliliği artırılabilir (Koshy, 2001; Vajda, 1989).

Standart Rastgelelik ve Güvenlik Testleri ile Değerlendirme: Algoritmanın çıktılarının rastgelelik ve entropi seviyesinin kriptografik standartlara uygunluğunun test edilmesi önemlidir. Bu doğrultuda, NIST SP 800-22 ve Diehard gibi test

takımları kullanılarak algoritmanın güvenlik profili daha doğru şekilde değerlendirilebilir.

Bu öneriler doğrultusunda yapılacak olan çalışmalar, Pell-Lucas tabanlı imza algoritmasının hem akademik olarak katkı düzeyini artıracak hem de uygulamaya yönelik sürdürülebilirliğini güçlendirecektir.

KAYNAKÇA

Battarbee, C., Kahrobaei, D., Perret, L., & Shahandashti, S. F. (2023, April 25). SPDH Sign: towards Efficient, Post quantum Group based Signatures. *arXiv*. https://arxiv.org/abs/2304.12900

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, 7–11.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography. Springer.

BTQ. (2025, February 26). One Shot Signatures: A New Paradigm in Quantum Cryptography. *BTQ Blog*. https://btq.com/blog/one-shot-signatures

Chavez Saab, J. et al. (2023, June 1). SQIsign: compact post quantum signatures from quaternions and isogenies. *Cryptology ePrint Archive*. https://eprint.iacr.org/2023/765

Chen, L., Chen, L.-K., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Cid, M. I. G., Martín, L. O., Martín, D. D., Sánchez Ledesma, R. M., Brito Méndez, J. P., & Martín Ayuso, V. (2023, March 1). A Feasible Hybrid Quantum Assisted Digital Signature for Arbitrary Message Length. *arXiv*. https://arxiv.org/abs/2303.00767

Çelik, S. Pell, Pell-Lucas, Jacobsthal ve Jacobsthal-Lucas sayılarında yeni tekrarlı bağıntılar (Master's thesis, Fen Bilimleri Enstitüsü).

Duman, M., & Duman, M. G. (2021). Encryption and decryption of the data by using the terms of the Lucas series. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 9(1), 1–7. https://doi.org/10.29130/dubited.825315

Knuth, D. E. (1997). *The Art of Computer Programming, Volume 1: Fundamental Algorithms* (3rd ed.). Addison-Wesley.

Koshy, T. (2001). Fibonacci and Lucas Numbers with Applications. John Wiley & Sons.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Mollin, R. A. (2006). An Introduction to Cryptography (2nd ed.). Chapman & Hall/CRC.

NIST (2023). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/post-quantum-cryptography

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th anniversary ed.). Cambridge University Press.

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

Prajapat, S., Jain, A., & Thakur, R. S. (2012). A novel approach for information security with automatic variable key using Fibonacci Q-Matrix. International Journal of Computer Communication and Technology, 3(3), 54–57.

Quantum Journal. (2023). Quantum Tokens for Digital Signatures. *Quantum*. https://quantum-journal.org/papers/q-2023-06-20-1055

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (20th anniversary ed.). Wiley.

Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books.

Stakhov, A. (2006). Fibonacci matrices, a generalization of the Cassini formula and a new coding theory. Chaos, Solitons & Fractals, 30(1), 56–66. https://doi.org/10.1016/j.chaos.2005.06.025

Stinson, D. R. (2006). Cryptography: Theory and Practice (3rd ed.). Chapman & Hall/CRC.

Tone, D. (2016). Report on Post-Quantum Cryptography. NIST IR 8105.

Vajda, S. (1989). Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications. Ellis Horwood Ltd.