NTRUEncrypt ve NTRUSign Tabanlı Kriptografi: Algoritma, Uygulama ve Güvenlik Analizi

Makbule Ozge Ozler
Yildiz Teknik Universitesi
Bilgisayar Muhendisligi Bolumu
Istanbul, Turkey
24501054

***Abstract*—NTRUEncrypt ve NTRUSign, modern kriptografinin temel taşlarından biri olan kafes tabanlı sistemlere dayanan, özellikle kuantum bilgisayar tehditlerine karşı dirençli olacak şekilde tasarlanmış şifreleme ve dijital imzalama algoritmalarıdır. Bu çalışmada NTRU tabanlı kriptografik sistemlerin teknik detayları, uygulama örnekleri ve güvenlik analizleri sunulmuştur. Java dilinde geliştirilen örnek uygulama üzerinden algoritmaların pratik analizleri gerçekleştirilmiş ve deneysel sonuçlarla desteklenmiştir.**

***Index Terms*—NTRUEncrypt, NTRUSign, post-kuantum kriptografi, dijital imza, lattice, Java uygulaması**

I. Giriş

Kriptografi, dijital çağın güvenlik ihtiyaçlarına çözüm sunmak amacıyla gelişen temel bilim dallarından biridir. Kuantum bilgisayarlar, klasik kriptografik algoritmalar üzerinde ciddi tehditler oluşturmakta, bu nedenle post-kuantum kriptografi önem kazanmaktadır. NTRU algoritmaları bu bağlamda öne çıkan yapılardır [1]–[3].

II. NTRUEncrypt Algoritmasinin Temelleri

A. Matematiksel Arka Plan

NTRU'nun temelinde, rasyonel sayıların cebirsel uzantısı olan $\mathbb{Z}_q[X]/(X^N - 1)$ halkası yer alır. Bu yapı, çembersel (dairesel) polinomları ifade eder. Tipik olarak p küçük bir asal sayı (örneğin 3), q ise daha büyük bir asal sayı (örneğin 2048) olarak seçilir.

Kullanılan polinomlar, çok az sayıda sıfır olmayan katsayıya sahip olacak şekilde seçilir; bu tür polinomlara sparse (seyrek) polinomlar denir. Örneğin, algoritmanın merkezinde yer alan halka şu şekilde ifade edilir:

$$R = \mathbb{Z}_q[X]/(X^N - 1) \tag{1}$$

Verilen bir halka R içinde şifreleme işlemi şu şekilde tanımlanır:

$$e = p \cdot r \cdot h + m \mod q \tag{2}$$

Bu yapı, hem rastgelelik hem de doğruluk sunar. Çözme işlemi yalnızca özel anahtara sahip olan tarafça yapılabilir.

B. Parametreler

NTRU algoritmasında güvenlik ve verimlilik, parametre seçimlerine bağlıdır. Temel parametreler:

- **N**: Polinom derecesi; halka elemanlarının sayısını belirler (örneğin 167, 251, 347).
- **p**: Küçük modül; genellikle 3 olarak seçilir.
- **q**: Büyük modül; genellikle 2048 veya 4096 gibi değerlerdir.

TABLE I
NTRUEncrypt Parametreleri ve Açiklamalari

Parametre	Açıklama
N	Polinom derecesi (halkanın boyutu)
p	Küçük bir asal sayı (genellikle 3)
q	Büyük bir modül (genellikle 2048, 4096 gibi)
df	Özel anahtarın katsayılarındaki +1 sayısı
dg	Rastgele polinomun (g) +1 sayısı
dr	Şifreleme sırasında kullanılan rastgele polinomun derecesi

Bu parametreler, algoritmanın hem performansını hem de güvenliğini doğrudan etkiler.

C. Anahtar Üretimi

Anahtar üretimi aşamasında, rastgele seçilmiş iki kısa polinom f ve g kullanılır. f, hem $\mod p$ hem de $\mod q$ altında terslenebilir olmalıdır. Açık anahtar, aşağıdaki şekilde hesaplanır:

$$h = p \cdot g \cdot f^{-1} \mod q \tag{3}$$

Özel anahtar ise f polinomudur.

D. Şifreleme

Şifreleme işlemi için rastgele bir kısa polinom r ve açık anahtar h kullanılarak aşağıdaki ifade oluşturulur:

$$e = r \cdot h + m \mod q \tag{4}$$

Burada m, mesajı temsil eden polinomdur.

E. Şifre Çözme

Şifreli metin e alındığında, özel anahtar f ile aşağıdaki işlem uygulanır:

$$a = f \cdot e \mod q \tag{5}$$

Daha sonra, a polinomu $\mod p$ altında işlenerek orijinal mesaj m elde edilir.

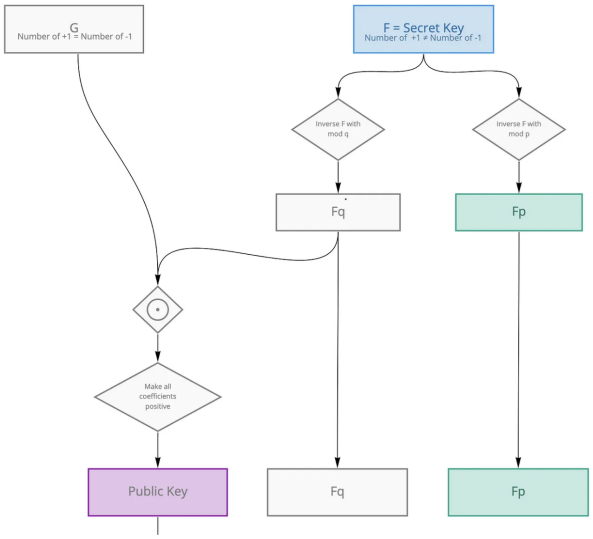

Fig. 1. Anahtar Uretimi Akis Diagrami

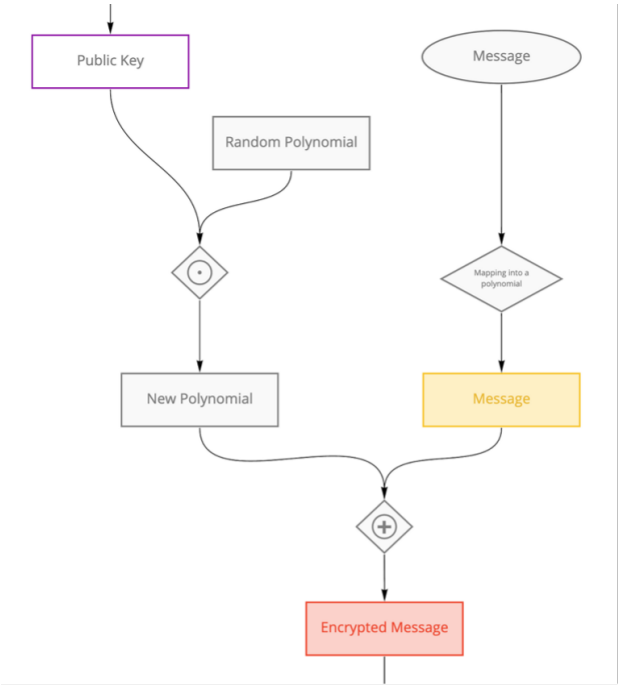

Fig. 2. Şifreleme Akis Diagrami

III. NTRUSign (İmza) Algoritmasının Temelleri

A. Dijital İmzanın Kriptografik Anlamı

Dijital imzalar, veri bütünlüğünü ve kimlik doğrulamasını sağlayan kriptografik yapılardır. Alıcı, imzalanmış verinin gerçekten göndericiye ait olduğunu doğrulayabilir.

B. NTRUSign Neye Dayanır?

NTRUSign algoritması, tıpkı NTREncrypt gibi halka yapısı ve kafes problemleri üzerine kuruludur. Ancak amacı

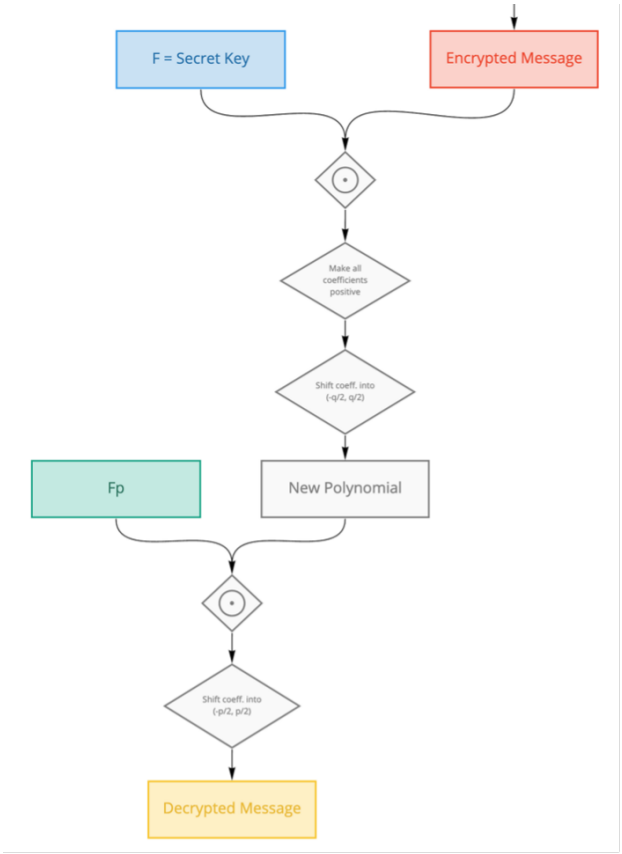

Fig. 3. Deşifreleme Akis Diagrami

şifreleme değil, dijital imza üretmektir. Temel yapı, kısa bir çözümün (polinomun) üretilmesi ve bu kısa çözümün doğrulanabilir olmasıdır. Gaussian sampling ve rejection sampling gibi tekniklerle istatistiksel izlerin azaltılması sağlanır.

C. NTRUSign Anahtar Üretimi

Özel anahtar genellikle kısa bir polinom çiftinden oluşur. Açık anahtar ise bu çift kullanılarak halka üzerinde belirli dönüşümlerle elde edilir.

D. İmzalama Süreci

Mesaj, hash fonksiyonu ile özetlenir. Bu özet yardımıyla halka yapısında kısa çözüm (polinom) oluşturulur. Bu kısa çözüm, imza olarak kullanılır.

E. Doğrulama Süreci

Doğrulama tarafı, gönderilen imzanın geçerli olup olmadığını halka üzerinde yapılan çarpım ve mod işlemleriyle kontrol eder. Eğer sonuç beklenen değere uygunsa imza geçerlidir.

F. Güvenlik Notu

NTRUSign'in erken sürümleri bazı güvenlik açıkları taşımaktaydı. Güncel versiyonlar Gaussian dağılımına göre örnekleme yaparak bu açıkları kapatmıştır. Ancak, uygulamada dikkatli rastgelelik kullanımı kritik önem taşır.

IV. NTRUSIGN VS NTRUENCRYPT

NTRUEncrypt gizliliği sağlarken, NTRUSign kimlik doğrulama amacına yöneliktir. Her iki algoritma da halka yapısını ve lattice problem temelli güvenlik varsayımlarını paylaşır.

TABLE II
NTRUENCRYPT VE NTRUSIGN KARŞILAŞTIRMASI

Özellik	NTRUEncrypt	NTRUSign
Kriptografik amaç	Gizlilik (confidentiality)	Kimlik doğrulama (authenticatio
Anahtar türü	Şifreleme anahtar çifti	İmza anahtar çifti
Operasyon	Şifreleme / Çözme	İmzalama / Doğrulama
Güvenlik temeli	Lattice problemi	Lattice tabanlı imza üretimi
Kullanım alanı	Mesaj/dosya şifreleme	Dijital belge imzalama

V. UYGULAMA ÖRNEĞI VE DENEYSEL TESTLER

Bu bölümde, Java dilinde geliştirilen bir uygulama üzerinden NTRUEncrypt ve NTRUSign algoritmalarının pratik performansı değerlendirilmiştir. Testler `SimpleExample.java` dosyası temel alınarak yürütülmüştür. [4]

A. Test Ortamı ve Yapı

Geliştirme ortamı: macOS, OpenJDK 23.0.2
Donanım: Apple M1, 8GB RAM
Kod: https://github.com/ozgeozler93/NtruEncryption-NtruSignature

B. Test 1: Şifreleme/Çözme Süresi

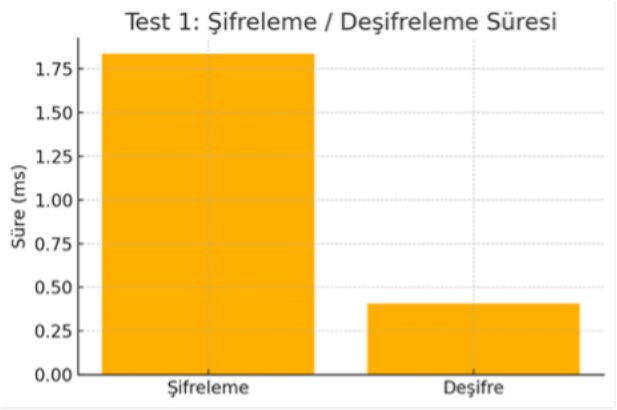

Fig. 4. Test 1: Şifreleme ve Deşifreleme Süreleri

Sonuçlar, şifreleme süresinin ortalama 1.835 ms, çözme süresinin ise 0.407 ms olduğunu göstermektedir.

C. Test 2: Rastgelelik Testi

Algoritma rastgelelik içermektedir, bu da güvenliği artıran önemli bir özelliktir.

D. Test 3: Parametre Kıyaslaması

Daha yüksek N değeri, işlem süresini artırırken güvenlik düzeyini de yükseltmektedir.

İmza süreci başarıyla tamamlanmış ve doğrulama geçerli sonuç vermiştir.

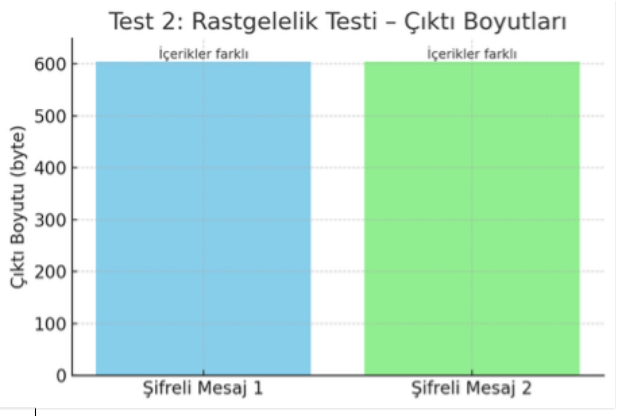

Fig. 5. Test 2: Rastgelelik Testi – Aynı mesaj, farklı şifreli çıktılar

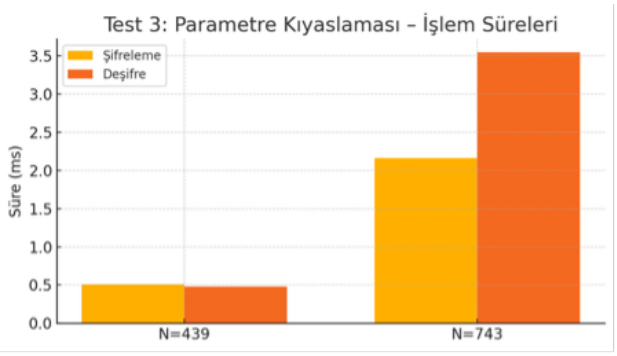

Fig. 6. Test 3: Parametre Setleriyle İşlem Süresi Karşılaştırması

E. Test 9: Avalanche Etkisi

Algoritma güçlü avalanche etkisi göstermektedir.

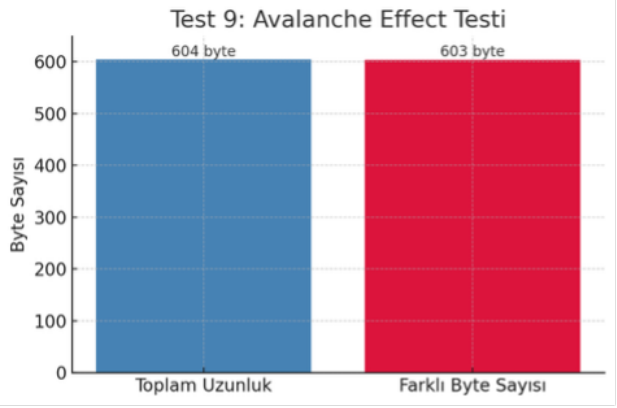

Fig. 7. Test 9: Avalanche Etkisi – Küçük giriş değişikliklerinin büyük çıktılar üretmesi

F. Test 12: Seri Şifreleme Performansı

100 ardışık şifreleme ortalaması 0.175 ms olarak ölçülmüştür.

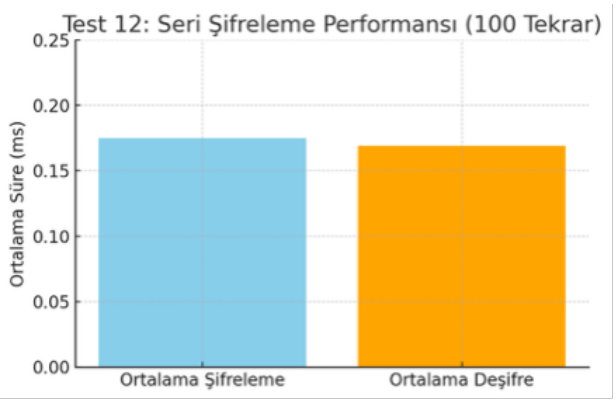

Fig. 8. Test 12: Seri Şifreleme Performansı – Ortalama süre analizi

VI. Avantajlar ve Dezavantajlar

A. NTRUEncrypt

Avantajlar:

- Kuantum sonrası güvenliğe sahiptir.
- Yüksek hız ve düşük gecikme sağlar.
- Kaynak kısıtlı cihazlarda kullanılabilir.
- Küçük anahtar boyutları sunar.

Dezavantajlar:

- Uzun mesajlarda sınırlı performans gösterir.
- Parametre seçimi hassasiyet gerektirir.
- Yan kanal saldırılarına karşı önlem alınmalıdır.

B. NTRUSign

Avantajlar:

- Post-kuantum güvenliği sağlar.
- Hızlı imzalama ve doğrulama süreçleri sunar.
- Kısa anahtar ve imza boyutlarıyla öne çıkar.

Dezavantajlar:

- Rastgelelik eksikliği özel anahtarı açığa çıkarabilir.
- Bazı varyantları istatistiksel zafiyet içermektedir.
- Modern varyantlara göre daha az tercih edilmektedir.

VII. Kullanim Alanlari

A. NTRUEncrypt Kullanım Alanları

- IoT cihazlarında ve kablosuz sensör ağlarında veri güvenliği.
- VPN ve TLS gibi protokollerde kuantum dirençli şifreleme. [5].
- Gömülü sistemlerde veri gizliliği.
- Bulut bilişim altyapısında uçtan uca veri koruma.

B. NTRUSign Kullanım Alanları

- Dijital belgelerin imzalanması.
- Elektronik oylama sistemleri.
- Yazılım güncellemelerinin bütünlük doğrulaması. [6]
- Blockchain tabanlı dijital kimlik altyapıları.

VIII. Güvenlik Analizi ve Saldırı Dayanımı

A. NTRUEncrypt Güvenlik Değerlendirmesi

NTRUEncrypt algoritması, matematiksel olarak SVP (Shortest Vector Problem) ve CVP (Closest Vector Problem) gibi zorluk seviyesi yüksek problemlere dayanmaktadır. Bu sayede kuantum algoritmalarıyla (örneğin Shor veya Grover) kolayca çözülemez. Ancak güvenlik, parametre seçimlerine oldukça duyarlıdır. Düşük kaliteli rastgelelik veya yanlış parametre kombinasyonları saldırıya açık kapı bırakabilir. Ayrıca, yan kanal saldırılarına karşı ek önlemler alınması gerekir.

B. NTRUSign Güvenlik Değerlendirmesi

NTRUSign teorik olarak kuantum sonrası güvenli olsa da, bazı varyantları geçmişte özel anahtara dair bilgiler sızdırmıştır. Bu sızıntılar, yeterince güçlü rastgelelik ve gizlilik sağlanmayan uygulamalardan kaynaklanmıştır. Bu nedenle Gaussian örnekleme, rejection sampling gibi güvenlik arttırıcı tekniklerin kullanılması önemlidir. Günümüzde BLISS, Falcon gibi daha güvenli alternatif imza sistemleri öne çıkmaktadır. Ancak doğru parametrelerle NTRUSign halen uygulanabilir bir çözümdür.

IX. Sonuç

Bu çalışma, NTRUEncrypt ve NTRUSign algoritmalarının post-kuantum kriptografi alanındaki teorik temellerini, pratik uygulamalarını ve güvenlik açıklarını sistematik bir şekilde incelemiştir. Deneysel testler, NTRUEncrypt'in kısa mesajlarda yüksek performans ve kuantum direnci sunduğunu, ancak uzun veri blokları için hibrit şifreleme modellerine ihtiyaç duyulduğunu ortaya koymuştur [6]. NTRUSign'in ise dijital imza doğrulamada hızlı sonuçlar ürettiği ancak bazı varyantlarının istatistiksel sızıntı riski taşıdığı belirlenmiştir [5]. Uzun mesajlar için AES-NTRU hibrit modelleri önerilmektedir. İmza algoritmalarında Falcon veya BLISS gibi daha güncel varyantlar tercih edilmeli, parametre optimizasyonu için NIST standartları takip edilmelidir [7].

References

[1] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," in *International Algorithmic Number Theory Symposium*. Springer, 1998, pp. 267–288.

[2] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "Ntru prime: Reducing attack surface at low cost," *IACR Cryptology ePrint Archive*, vol. 2017, p. 565, 2017.

[3] N. I. of Standards and Technology, "Nistir 8413: Status report on the third round of the nist post-quantum cryptography standardization process," NIST, Tech. Rep., 2022.

[4] tbuktu, "Simpleexample.java," GitHub, 2018, https://github.com/tbuktu/ntru.

[5] J. Buchmann, E. Dahmen, and M. Schneider, "Post-quantum cryptography: State of the art," in *PQCrypto*. Springer, 2009, pp. 1–13.

[6] Y. Wang and C. Wang, "On the hardness of the ntru problem and its applications," *Information Sciences*, vol. 589, pp. 21–37, 2022.

[7] E. Alkim, L. Ducas, T. P"oppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in *25th USENIX Security Symposium*, 2016, pp. 327–343.