All Sciences Proceedings

5th International Conference on Applied Engineering and Natural Sciences

July 10-12, 2023 : Konya, Turkey

All Sciences Proceedings
http://as-proceeding.com/

https://www.icaens.com/

NTRU Anahtar Kapsülleme Mekanizması İçin Uygulamaya Özel İşlemci Tasarımı

Latif Akçay* ve Mustafa Alptekin Engin

Elektrik-Elektronik Mühendisliği, Bayburt Üniversitesi, Türkiye

(lakcay@bayburt.edu.tr)

Özet – Kuantum Sonrası Kriptografi son yıllarda oldukça aktif araştırma alanlarından biri haline gelmiştir. Kuantum çağına uygun, güvenli ve çok geniş bir uygulama alanında kullanıma uygun anahtar paylaşım mekanizmaları ve dijital imza algoritmaları tüm insanlık için kritik ihtiyaçlardandır. Buna yönelik olarak NIST tarafından organize edilen standartlaştırma süreci halen devam etmektedir. Sürecin final aşamasına kadar ulaşan aday anahtar kapsülleme mekanizmalarından birisi de bu alanda bilinen en eski algoritmalarından olan NTRU'dur. Tam sayı kafesler üzerinde tanımlanan En Kısa Vektör Problemi ile kurgulanan NTRU algoritması kuantum sonrası haberleşme sistemleri için hızlı ve güvenli bir alt yapı sunmaktadır. NTRU ile hem klasik bilgisayarlar hem de kuantum bilgisayarlarla yapılabilen ataklara karşı dayanıklı ve ölçeklendirilebilir bir anahtar paylaşım sistemi tasarlanabilir. Ancak bir algoritmanın teorik olarak başarılı olması onun pratik anlamda da uygulanabilir olması anlamına gelmez. Bir algoritmanın dijital sistemlerde kullanılabilir olması için yeterince yüksek performanslı ve verimli olarak çalıştırılabilmesi gerekir. Kriptografi uygulamaları gömülü sistemlerde de yaygın olarak kullanılmaktadır. Bu nedenle Kuantum Sonrası Kriptografi algoritmalarının hızlı ve verimli bir şekilde çalışmasını sağlayacak donanım hızlandırıcılar geliştirilmelidir. Bu çalışmada, NTRU için tasarlanmış, Taşıma Tetiklemeli Mimari işlemcilerde kullanılabilecek donanım hızlandırıcılar önerilmektedir. Ayrıca bu komutların eklendiği 64-bit işlemci tasarımı performans, enerji tüketimi ve yonga alanı açısından endüstride yaygın olarak kullanılan RISC-V mimarili işlemcilerle karşılaştırılmaktadır.

Anahtar Kelimeler – Kuantum Sonrası Kriptografi, Kafes Temelli Kriptografi, NTRU, RISC-V, Uygulamaya Özel İşlemci Tasarımı, Taşıma Tetiklemeli Mimari, FPGA.

I. GİRİŞ

Kuantum bilgisayarlar, birçok araştırma alanında insanlığın yeni teknolojiler geliştirmesine öncülük edecek sistemlerdir. Üstün hesaplama yetenekleri sayesinde uzay araştırmaları, kimyasal sentezler, iklim araştırmaları ve veri analizi gibi daha pek çok alanda kuantum bilgisayarların kritik kazanımlar sağlayacağı öngörülmektedir [1]. Önceki yıllarda daha çok teorik araştırmalar boyutunda olan kuantum bilgisayar geliştirme çalışmaları özellikle son yıllarda ciddi ivme kazanmıştır. Çok sayıda devlet, geniş ölçekli firmalar ve hatta pek çok yeni girişim kuantum bilgisayar geliştirme projeleri yürütmektedir [2].

Kuantum hesaplama teknolojisinin insanlığa sağlayacağı faydaların yanı sıra bir takım yeni tehditlere sebep olacağı da bilinmektedir. Bunların en önemlilerinden biri de bilgi güvenliği alanında kendini göstermektedir. Günümüzde kullanılan haberleşme sistemlerinin güvenliği kriptografi algoritmalarıyla sağlanmaktadır. Bu algoritmalar ise bilinen en hızlı klasik bilgisayarın bile uzun bir süre boyunca deneme-yanılma gibi yöntemlerle çözümünü bulamayacağı matematiksel problemlere dayanılarak kurgulanmıştır [3]. Bu sayede, şifreli veriler bir şekilde ele geçirilmiş olsa bile, güvenli bir bilgi iletişimi mümkün kılınmaktadır. Ancak kuantum mekaniğinin dayandığı süper pozisyon ilkesine göre hesaplama yapan bilgisayarlar için bazı problemlerin çözümü klasik bilgisayarlara oranla çok kısa sürebilmektedir [4]. Özellikle günümüzde çok yaygın olarak kullanılan açık

anahtarlı (asimetrik) şifreleme sistemlerinin dayandığı tam sayı faktörizasyonu ve ayrık logaritma problemleri klasik bilgisayarlara karşı güvenli olmasına karşın kuantum bilgisayar ataklarına karşı zayıftır. Bu tehlikeye ilk kez Amerikan matematikçi Peter Shor dikkat çekmiş ve bu problemlerin çözümünü hızlandırabilen bir kuantum bilgisayar algoritması geliştirmiştir [5]. Bunun anlamı, yeterince gelişmiş bir kuantum bilgisayara sahip olan herhangi birinin Peter Shor'un gösterdiği yöntemle yaygın ve güçlü algoritmaları etkili bir zamanda kırabilmesidir. Henüz bunu yapabilecek bir kuantum bilgisayar olmadığı ve yakın gelecekte de olmayacağı varsayımı altında bile bu tehdit hala geçerlidir. Çünkü günümüzde toplanan veriler ilerleyen yıllarda çözümlenmek üzere saklanabilir.

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST) 2016 yılında hem klasik hem de kuantum bilgisayar ataklarına karşı dayanıklı, yaygın olarak kullanılabilir, yeni nesil asimetrik şifreleme yöntemleri bulmak ve standartlaştırmak için uluslararası bir süreç başlatmıştır [6]. Sürecin amacı tek bir kazanan algoritma bulmak değil, farklı alanlar için çeşitli alternatifler oluşturmak ve bunların standartlarını tanımlamaktır.

Kafes Temelli Kriptografi yöntemleri Kuantum Sonrası Kriptografi için en umut vadeden alanlar arasındadır [7]. Nitekim NIST tarafından yürütülen sürecin üçüncü aşamasına kalan toplam 7 adaydan 5 tanesi Kafes Temelli Kriptografi tekniklerine dayanmaktadır. Bunlardan biri de Nth Degree Truncated Polynomial Ring Units (NTRU) anahtar kapsülleme mekanizmasıdır [8].

Çok Uzun Buyruk Kelimesi (Very Long Instruction Word Length - VLIW) mimarisinin bazı zayıf yanlarının giderildiği bir türevi olan Taşıma Tetiklemeli Mimari (Transport - Triggered Architecture - TTA), komut seviyesinde paralel hesaplama ve özelleştirilebilir işlevsel birimleri öne çıkaran bir işlemci tasarım felsefesidir [9]. Açık kaynak kodlu ve ücretsiz bir araç seti olan TTA-based Co-Design Environment (TCE) [10] ile modelleme, kod derleme, donanımla uyumlu fonksiyonel benzetim, kaynak kullanım analizi ve hatta donanım kodu üretimi gibi tüm işlemci tasarım süreçleri gerçekleştirilebilir.

Bu çalışmada NIST Kuantum Sonrası Kriptografi Standartlaştırma Süreci finalistlerinden olan NTRU anahtar kapsülleme mekanizması için TTA temelli bir işlemci tasarımı yapılmıştır. İkinci bölümde sırasıyla NTRU algoritması ve TTA mimarisi kısaca tanıtılmıştır. Üçüncü bölümde işlemci tasarım yöntemi detaylıca açıklanmış, yapılan testler ve elde edilen sonuçlar aktarılmıştır. Beşinci bölümde ise tüm çalışmanın genel bir değerlendirmesi yapılmış ve önümüzdeki dönem yapılacak olan çalışmalara değinilmiştir.

II. NTRU VE TTA

Bu bölümde çalışmanın temellerini oluşturan anahtar kapsülleme mekanizması ve işlemci mimarisi ile ilgili temel bilgiler sunulmuştur.

A. NTRU

NTRU, tüm polinom katsayıları tam sayılarla ifade edilen bir halka üzerinde tanımlanır ($R = Z[x](x^n - 1)$. Sistem parametreleri aralarında asal pozitif tam sayılar (n, p, q) ve polinom kümeleri ile verilir. Anahtar üretimi için öncelikle halka üzerinde f ve g polinomları üretilir. Burada f için ilave şart hem p hem de q için terslenebilir olmasıdır $(f.f_p = 1\ (mod\ p), f.f_q = 1\ (mod\ q))$. Bu koşula uygun polinomlar üretildiğinde alıcının gizli anahtarları f ve f_p olarak belirlenmiş olur. Sistemin açık anahtarı h ise (1)'de verildiği gibi hesaplanır.

$$h = p.f_q.g\ (mod\ q) \qquad (1)$$

Gönderici halka içerinde bir polinom formatına dönüştürdüğü bir m mesajını göndermek için rastgele oluşturulan r polinomu ile (2)'de verilen işlemi yapar.

$$c = r.h + m\ (mod\ q) \qquad (2)$$

Alıcı taraf kendisine gönderilmiş olan şifreli c mesajını (3) ve (4) ile çözerek orijinal mesajı elde etmiş olur. Ancak burada verilen işlemler sadece algoritmanın temel operasyonudur. NIST sürecine sunulan resmi algoritma bilinen bazı atak yöntemlerine karşı gereksinimleri karşılamak için ek işlemler içermektedir. Bu çalışmada söz konusu resmi algoritma ve önerilen referans C yazılım kodu kullanılmıştır [8].

$$a = f.c\ (mod\ q),\ b = a\ (mod\ p) \qquad (3)$$

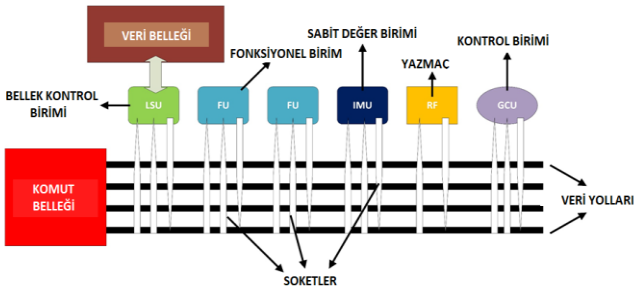
$$d = f_p.b\ (mod\ p) = f_p.f.m\ (mod\ p) = m \qquad (4)$$

B. TTA

TTA, işlenecek verilerin çoklu paralel veri yolu üzerinden fonksiyonel birimler arasında taşınması mantığıyla kurgulanan bir mimaridir. Sisteme özel bir fonksiyonel birim olarak bağlanan kontrol birimi iş akışını yönetir. Veri belleği ise yine özel bir fonksiyonel birim tarafından kontrol edilir. VLIW mimarisinden farklı olarak yazmaç bloğu da sistem üzerinde sıradan bir fonksiyonel birimdir. Tasarımcı tüm fonksiyonel birimleri ve paralel veri yollarını uygulama ihtiyaçlarına göre özelleştirebilmektedir. Veri hatlarının sayısı ve genişliği, fonksiyonel birimlerin içerdiği işlemler, bu işlemlerin her birinin kaç saat döngüsünde tamamlanacağı gibi tüm parametreler tasarımcının kontrolündedir.

TTA kod çalıştırma yönteminde zamanlama (scheduling) derleyici tarafından belirlenir ve statiktir. Bu sayede kontrol biriminin donanımsal tasarımında karmaşıklığın azaltılması sağlanır.

TTA işlemcilerde işlenen veriler bir yazmaç bloğunda saklanmak yerine sıradaki işleme sokulacağı fonksiyonel birime doğrudan taşınır. Bu sayede mecbur kalınmadıkça yazmaç bloğu kullanılmaz. Bu yöntemle güç tüketimi azaltılır ve veri iletim yükü düşürülür. TTA işlemcilerin genel yapısı Şekil 1'de sunulmuştur.



Şekil 1. TTA mimarili işlemcilerin genel yapısı.

III. İŞLEMCİ TASARIMI

Tasarımın tüm aşamaları TCE aracı kullanılarak yapılmıştır. Öncelikle NTRU algoritma yazarları tarafından hazırlanan ve NIST sürecine sunulan referans C kodu, TCE ile sunulan basit bir 32-bit işlemci için derlenmiştir. Fakat NTRU algoritması 64-bit değerler üzerinde hesaplamalar yaptığı için kodun 32-bit TTA işlemcisi üzerinde çalıştırılamaz olduğu görülmüştür. Bu nedenle [11]'de kullanılan teknikler uygulanarak 64-bit temel işlemci tasarımı yapılmıştır. TCE'nin işlemci modelleme aracı olan ProDe üzerinde yapılan bu tasarım TTA64 olarak adlandırılmıştır. Bu aşamada fonksiyonel birimleri oluşturan tüm operasyonlar standart TCE komutları olduğundan ek bir donanım tasarımı yapılmamıştır. Hâlihazırda HDB aracında bulunan VHDL kodları TTA64 için düzenlenmiş ve daha sonra ProGe aracı kullanılarak sentezlenebilir işlemci tasarımı üretilmiştir. Ardından bu tasarım Xilinx Vivado ile xc7a100t FPGA platformu için gerçeklenmiştir. Tablo 1'de TTA64 için elde edilen kaynak tüketim değerleri popüler 64-bit RISC-V işlemcilerle karşılaştırılmaktadır. Burada yapılan kıyasın sadece eş işlevsellikler sağlayan işlemci çekirdekleri için yapıldığına ve çevresel birimleri (UART, SPI, gibi) içermediğine özellikle dikkat edilmelidir.

Tablo 1. TTA ve RISC-V mimarili işlemci çekirdeklerinin FPGA kaynak kullanımları.

İşlemci	Frekans	LUT, FF, DSP	Güç(mW)
TTA64	52 MHz	4725, 3270, 6	115
TTA64N	45 MHz	8455, 5610, 8	124
Rocket [12]	62 MHz	7693, 4330, 4	141
CVA6 [13]	40 MHz	9567, 4729, 16	122

NTRU referans kodu TTA64 ve RISC-V işlemci platformları için ayrı ayrı derlenmiştir. Daha sonra tüm işlemcilerde anahtar üretimi, şifreleme ve şifre çözme işlemleri için harcanan toplam saat döngüsü değerleri elde edilmiştir. Tablo 2'de bu değerler 3 farklı NTRU parametre seti için verilmektedir [8].

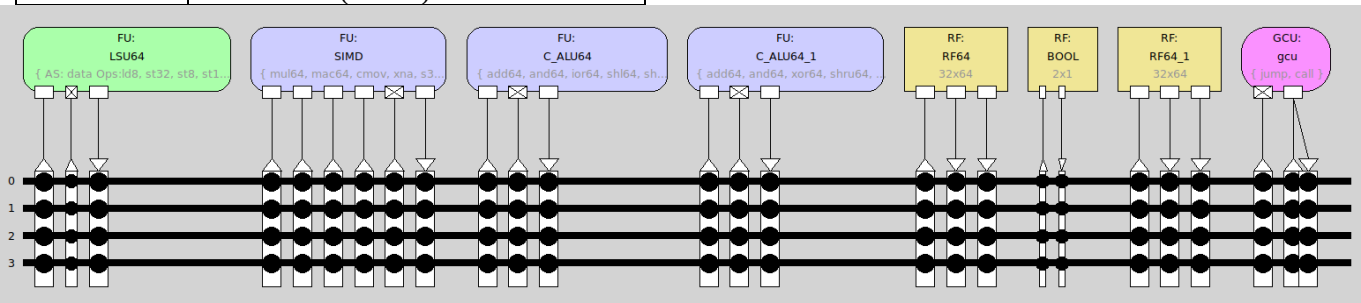
Tablo 2. Üç farklı NTRU parametre seti için toplam saat döngüsü sayısı (değerler milyon mertebesinde verilmiştir).

Parametre	TTA64	TTA64N	Rocket	CVA6
HRSS701	94.06	68.75	168.22	186.27
HPS2048509	50.05	--	91.81	105.48
HPS2048677	82.08	--	161.74	185.47

TTA64 ile elde edilen başarımı artırmak için özel komut tasarımları yapılmıştır. Bunun için öncelikle TCE'nin saat döngüsü uyumlu benzetim aracı olan Proxim üzerinde yapılan analizler sonucunda algoritmanın en sık tekrarlanan işlemleri ve ayrıca darboğaza düşülen bölümleri tespit edilmiştir. Bu noktada bir tasarım önceliği olarak frekans değerinin düşmesine sebep olmayacak kadar az karmaşık komutlar tercih edilmiştir. Geliştirilen yeni komutlar TCE'nin Osed operasyon kümesine eklenmiştir. Daha sonra bu komutlar mevcut işlemci tasarımına eklenerek yeni fonksiyonel birimler oluşturulmuştur. Tablo 3'de söz konusu komutlar gerçekleştirdikleri işlemlerle birlikte sunulmaktadır.

Tablo 3. NTRU algoritması için geliştirilen TTA komutları (I = giriş, O = çıkış, C=sabit değerler).

Komut Adı	İşlem
ANDXOR	O = I1 & (I2 ^ I3)
TZ3TZQ	(C2 & ((I1 & C1) ^((I2 & C1) >>C3)))
V0CAL	O = (I1 + I2) >> C – I3
V1CAL	O = I1 – (I2) << C1 – (I3) << C2
V2CAL	O = ((C1 x I1 – I2) >> C2) – I3
XNA	O = I1 ^ (~I2 & I3)
ROL	O = (I1 << I2) ^ (I1 >> (C – I2))
MOD3U8	O = I1 % C1



Şekil 2. TTA64N işlemcisinin TCE-ProDe aracında tasarlanan fonksiyonel birimleri.

Tasarlanan yeni işlemci modeli TTA64N olarak adlandırılmıştır. Platformun ProDe modeli Şekil 2'de verilmiştir. Tasarımı olgunlaştırıldıktan sonra yeni birimlerin donanım tasarımı VHDL ile yapılmıştır. Vivado ile sentez ve implementasyon işlemlerinin ardından elde edilen kaynak tüketimi ve frekans değerleri Tablo 1' de sunulmuştur.

TTA64N işlemcisi NTRU- HRSS701 referans kodu ile test edilmiştir. Elde edilen toplam saat döngüsü değerleri Tablo 2 'de diğer platformlarla birlikte paylaşılmıştır. Veriler incelendiğinde eklenen komutların saat döngüsü sayısı cinsinden performansı yaklaşık olarak %28 artırdığı görülmüştür. Frekans değerindeki kısmi düşüşe rağmen başarım artışı yaklaşık %25 olarak gerçekleşmiştir. RISC-V mimarili işlemciler ile kıyaslandığında ise TTA64N platformunun toplam çalışma süresi açısından en az 1.9 kat daha hızlı olduğu görülmüştür.

IV. SONUÇ

Bu çalışmada NIST Kuantum Sonrası Kriptografi Standartlaştırma Süreci üçüncü aşama adaylarından NTRU algoritması için TTA temelli uygulamaya özel işlemci tasarımı yapılmıştır. Algoritmanın çalışma süresini düşürmek ve verimliliği artırmak için yeni operasyonlar tasarlanmıştır. Daha sonra bu özel komutlar önceden tasarlanmış 64-bit temel işlemci tasarımına bazı ilave fonksiyonel birimlerle entegre edilmiştir. Geliştirilen platformla referans NTRU C kodu test edilmiştir. Sonuçta hem performans, hem gerekli yonga alanı, hem de toplam enerji tüketimi açısından popüler RISC-V işlemcilere göre daha iyi sonuçlar elde edilmiştir. Bu bağlamda, TTA mimarisinin özellikle gömülü sistemlerde Kuantum Sonrası Kriptografi uygulamaları için uygun bir işlemci tasarım yöntemi olduğu söylenebilir. Elde edilen değerlerin daha fazla özelleştirme yapılarak geliştirilmesi de mümkündür. Gelecek çalışmalarda NTRU'nun diğer parametre setleri için de TTA64N üzerinde testler ve özelleştirmeler yapılacaktır.

KAYNAKLAR

[1] Alexeev, Yuri, et al. "Quantum computer systems for scientific discovery." *PRX Quantum* 2.1 (2021): 017001.

[2] Alberts, Garrelt JN, et al. "Accelerating quantum computer developments." *EPJ Quantum Technology* 8.1 (2021): 18.

[3] Hellman, Martin E. "An overview of public key cryptography." *IEEE Communications Magazine* 40.5 (2002): 42-49.

[4] Ladd, Thaddeus D., et al. "Quantum computers." *nature* 464.7285 (2010): 45-53.

[5] Shor, Peter W. *"Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer."* SIAM review 41.2 (1999): 303-332.

[6] Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology, 2016.

[7] Micciancio, Daniele, and Oded Regev. *"Lattice-based cryptography." Post-quantum cryptography.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. 147-191.

[8] Chen, Cong, et al. "Algorithm specifications and supporting documentation." *Brown University and Onboard security company, Wilmington USA* (2019).

[9] Akcay, Latif, and Berna Ors. "Custom TTA Operations for Accelerating Kyber Algorithm." *2021 13th International Conference on Electrical and Electronics Engineering (ELECO)*. IEEE, 2021. doi: 10.23919/ELECO54474.2021.9677863.

[10] Akcay, Latif, and Yalçın, S.B.Ö. "Comparison of RISC-V and transport triggered architectures for a post quantum cryptography application." *Turkish Journal of Electrical Engineering and Computer Sciences* 29.1 (2021): 321-333. https://doi.org/10.3906/elk-2003-27

[11] Akçay, Latif, and Berna Örs Yalçın. "Analysing the potential of transport triggered architecture for lattice-based cryptography algorithms." *International Journal of Embedded Systems* 15.5 (2022): 404-420. https://doi.org/10.1504/IJES.2022.127164.

[12] Asanovic, Krste, et al. "The rocket chip generator." *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2016-17* 4 (2016): 6-2.

[13] Zaruba, Florian, and Luca Benini. "The cost of application-class processing: Energy and performance analysis of a Linux-ready 1.7-GHz 64-bit RISC-V core in 22-nm FDSOI technology." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 27.11 (2019): 2629-2640.