T.C
SAHA İSTANBUL & TÜBİTAK TÜSSİDE
SAHA AKADEMİ MBA YÖNETİCİ GELİŞTİRME PROGRAMI

IOT Cihazlarında Post Quantum Kriptografi Kullanımı

MBA Proje
Onur İŞLER

Danışman
Dr. Uğur TARÇIN
Ankara- 2025

ARAŞTIRMA PROJESİ UYGUNLUK FORMU

MBA: 2024-2025/77

1. SAHA İstanbul Yönetim Kurulu kararıyla, 2024-2025 eğitim döneminden itibaren SAHA AKADEMİ MBA katılımcılarına "Araştırma Projesi" hazırlama yükümlülüğü getirilmiştir. Bu uygulama; katılımcıların sektörel bilgi, stratejik düşünme ve akademik üretkenlik yetkinliklerini geliştirmeyi hedeflerken, savunma sanayii ekosistemine bilimsel katkıyı artırmayı amaçlamaktadır. Bu girişim, Türk savunma sanayii ekosisteminde bilimsel katkıyı artırmaya yönelik önemli bir adımdır.

2. SAHA İstanbul-SAHA AKADEMİ tarafından yayımlanan bu çalışma, ilgili yazar tarafından özgün biçimde hazırlanmış ve beyan edilmiştir. Çalışmada yer alan görüşler yazara ait olup, SAHA İstanbul'un kurumsal görüşünü yansıtmamaktadır. İçerikte sunulan bilgi, yorum ve sonuçların doğruluğu sorumlu yazara aittir. SAHA AKADEMİ; benzerlik oran tespitini yapmıştır.

3. Bu çalışma, [Onur İŞLER] tarafından hazırlanmıştır. Araştırma Projesi danışman tarafından değerlendirilmiş ve sunumu [25 Mayıs 2025] tarihinde yeterli görülerek kabul edilmiştir.

Araştırma Projesi Sunum Jüri Üyeleri

Başkan	Dr. Uğur Tarçın (*SAHA AKADEMİ Öğr.Görevlisi)*	*e-imzalıdır*
Üye	İlker Özkan (*Genel Sekreter Yrdc*)	*e-imzalıdır*
Üye	Pınar Erguvan Kaya (*SAHA İstanbul Kurumsal İlişkiler Müdürü)*	*e-imzalıdır*

(Formun aslı, imzalı olarak ilgili dosyada muhafaza edilmektedir.)

İÇİNDEKİLER

IOT CİHAZLARINDA POST QUANTUM KRİPTOGRAFİ KULLANIMI (PROJE)

Onur İŞLER

Türktrust

onurrislerr@gmail.com / onurisler@windowslive.com

Özet

Bu çalışma, kuantum sonrası dönemin bilgi güvenliğine etkilerini göz önünde bulundurarak, sınırlı kaynaklara sahip IoT cihazlarında post-kuantum kriptografi (PQC) algoritmalarının uygulanabilirliğini araştırmayı amaçlamaktadır. Geleneksel eliptik eğri kriptografisi (ECC) ile performans, güvenlik ve kaynak kullanımı açısından karşılaştırmalı bir değerlendirme yapılacaktır. Proje kapsamında Kyber, Dilithium ve SPHINCS+ gibi önde gelen PQC algoritmaları mikrodenetleyici tabanlı donanımlar üzerinde test edilerek, IoT sistemlerine entegrasyon potansiyelleri analiz edilecektir.

Waterfall modeli esas alınarak yürütülecek olan proje sürecinde; gereksinim analizi, algoritma seçimi, sistem tasarımı, prototipleme, entegrasyon ve test aşamaları sistematik bir şekilde ele alınacaktır. Testlerde NIST onaylı doğrulama yöntemleri kullanılacak, elde edilen veriler performans ve güvenlik kriterleri açısından karşılaştırmalı olarak raporlanacaktır.

Proje çıktıları, hem akademik camia hem de kamu ve özel sektör kuruluşları için bilimsel ve pratik katkı sağlamayı hedeflemektedir. Özellikle IoT sistemleriyle çalışan askeri ve sivil kuruluşlara, kuantum güvenli mimarilere geçişte rehberlik edecek nitelikte sonuçlar sunulması amaçlanmaktadır.

1. Proje Amacı

Bu projenin temel amacı, nesnelerin interneti (IoT) cihazlarında post-kuantum kriptografi (PQC) algoritmalarının uygulanabilirliğini araştırmak, bu algoritmaları geleneksel eliptik eğri kriptografisi (ECC) ile karşılaştırmak ve performans, güvenlik ile kaynak tüketimi açısından kapsamlı bir değerlendirme sunmaktır. Kuantum bilgisayarların gelişimi, özellikle ECC ve RSA gibi günümüzde yaygın olarak kullanılan kriptografik algoritmaların uzun vadede güvenliğini

tehdit etmektedir. Bu durum, hem kişisel kullanım alanlarına kadar yayılmış olan IoT cihazlarının hem de askeri ve endüstriyel uygulamalarda kullanılan gömülü sistemlerin siber güvenliğini risk altına sokmaktadır.

Günümüzde IoT cihazları düşük maliyetleri, taşınabilir yapıları ve enerji verimliliği nedeniyle yaygınlaşmakta; ev otomasyon sistemlerinden sağlık teknolojilerine, endüstriyel üretim hatlarından savunma sanayine kadar pek çok alanda kullanılmaktadır. Ancak bu cihazların sınırlı işlem gücü ve enerji kapasitesi, geleneksel kriptografik algoritmaların etkin biçimde uygulanmasını zorlaştırmaktadır. Aynı zamanda, bu cihazların internet üzerinden veri alışverişi yaparken üçüncü taraflarca müdahaleye açık hale gelmesi, mesajların gizliliği, bütünlüğü ve kimlik doğrulamasının güvenilir biçimde sağlanmasını kritik hâle getirmektedir.

Proje kapsamında, hafif yapılı, düşük kaynak tüketimli ve kuantum dirençli PQC algoritmalarının seçimi yapılarak IoT ortamlarında kullanılabilirliği değerlendirilecektir. Bu algoritmaların mesaj güvenliği, veri bütünlüğü, kimlik doğrulama ve gizlilik sağlama gibi temel güvenlik işlevlerini ne ölçüde yerine getirebildiği; işlem süresi, bellek kullanımı ve enerji tüketimi gibi metrikler üzerinden incelenecektir. Ayrıca proje kapsamında en uygun PQC algoritmasının seçilmesine yönelik prototip bir sistem geliştirilerek, kriptografik işlemlerin (imzalama, doğrulama, şifreleme, şifre çözme) IoT cihazları üzerinde kuantum güvenli biçimde gerçekleştirilmesi hedeflenmektedir.

Bu bağlamda proje, hem mevcut güvenlik tehditlerine karşı dirençli yeni nesil kriptografik çözümlerin geliştirilmesine katkı sağlamayı, hem de sınırlı kaynaklara sahip gömülü sistemlerde yüksek güvenlik gereksinimlerinin nasıl sağlanabileceğine yönelik uygulanabilir öneriler sunmayı amaçlamaktadır.

2. Projenin Kapsamı

- IoT cihazlarında kullanılan mevcut ECC tabanlı güvenlik çözümlerinin örnek analizi yapılacaktır.
- Post-quantum algoritmaların (Kyber, Dilithium, SPHINCS+) IoT cihazlarında uygulanabilirliği analiz edilecektir.
- Post-quantum algoritmaların IoT tabanlı sistemlere entegrasyonu çalışılacaktır.

- ECC ile post-quantum kriptografi çözümlerinin karşılaştırılması yapılacaktır.
- Mikrodenetleyici (STM32 gibi) tabanlı testler ve optimizasyon çalışmaları yapılacaktır.

3. Projenin Hedef Kitlesi

Proje öncelikle akademik çalışmalar için veri niteliğinde değer taşımaktadır. Bu çalışma ile literature katkı sağlarken yapılacak ileri düzey çalışmalara da başlangıç olması hedeflenmektedir. Bu sebeple hedef kitlesi arasında akademisyenler ve akademik çalışma yapmak isteyen lisans üstü öğrenciler bulunmaktadır. Projenin çıktıları ile IoT sistemlerin güvenli haberleşmesine ihtiyaç duyan, IoT sistemleri üzerine çalışmalar yapan askeri ve sivil teknoloji şirketleri, sivil toplum kuruluşları, kamu kurumları da ulaşmaya hedeflenen organizasyonlardır.

4. Projenin Yöntemi ve Çalışma Planı

a. Proje Yönetimi: Projede Waterfall yazılım yaşam döngüsü kullanılacaktır. Bu yaşam döngüsünde gereksinim ve analiz, tasarım, kodlama, entegrasyon, test çalışmaları yapılacaktır. Projenin her aşamasında gerekli dokümanlar oluşturularak düzenli güncellenecek ve versiyon takibi yapılacaktır. İş takibi açısından oluşturulan iş dağılım ağacı vasıtasıyla kritik yol takibi yapılırken, risk ve fırsat kontrolleri proje süresi boyunca belirlenen kilometre taşlarında takip dilecektir. Bu aşamada Proje Yönetim Planı, İş Dağılım Ağacı dokümanları üretilecektir.

b. Analiz - Fikir Üretim ve Tarama: Literatür araştırmaları ile birlikte projede yeni yöntemler geliştirebilmek için; son gelişmeler, konu ile ilgili otoriteler, haberler, post - kuantum konusu hakkında çalışan/çalışabilecek firmaların konuyla ilgili ürünlerinin takibi yapılarak geliştirilecek sistemin yetkinliğinin artırılması sağlanacaktır. Benzer ürünler ve piyasa araştırması sırasında SWOT (GZFT: GüÇLÜ Yönler, Zayıf Yönler, Fırsatlar ve Tehditler) analizi yapılarak, elde edilecek veriler ile pazar hakimiyeti sağlayacak fırsatlar değerlendirilecektir. Bu aşamada uygun cihaz araştırması yapılarak uygun algoritma uygun cihaz kombinasyonu üzerine durulacaktır. Bu aşamada Yazılım Gereksinim Dokümanı üretilerek analiz kararlarını içerecektir.

c. Tasarım-Geliştirme-Entegrasyon-Test: IoT sistemlerind çalışabilecek verimli PQC algoritmasının prototiplenmesi ve karşılaştırılmaları yapılacaktır. Ayrıca prototip ürün entegrasyon aşamasının sonundan itibaren performans değerleri belirlenen başarı hedeflerine göre Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve takip edilecek yayınlarda belirtilen yöntemlerle ölçülecektir. Testler için NIST veri modelleri ve NIST'in algoritma doğrulama

programına göre hazırlanan yöntemler kullanılacaktır. Bu yöntemlerden elde edilen veriler ile bilimsel makalelerden elde edilen veriler karşılaştırmalı olarak analiz edilerek raporlanacaktır. Bu aşamada asarım Dokümanı, Entegrasyon Planı, Test Planı Dokümanı üretilecektir.

d. Teknik danışmanlık ve iş birlikleri: IoT sistemlerde kullanılacak algoritmalar küresel çapta araştırmaları devam eden bir alan olduğundan akademik danışmanlık verebilecek akademisyenler araştırılarak danışmanlık sözleşmesi imzalanacaktır.

Projenin detaylı iş planı ve paketleri ek olarak "Ek'teki proje önerisi iş takvimi.xlsx" adlı dokümanda mevcuttur.

Resim 1. İş Planı ve Paketleri

	PROJE SÜRESİ TOPLAM SÜRE	BAŞLANGIÇ ZAMANI (T0) + 14AY																	
	DÖNEMLER	2025/2						2026/1						2026 /2					
	AYLAR	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
	PROJE SÜRESİ	T0+1	T0+2	T0+3	T0+4	T0+5	T0+6	T0+7	T0+8	T0+9	T0+10	T0+11	T0+12	T0+13	T0+14				
1. Analiz		1	2	3	4														
	1.1 Algoritma araştırması ve analiz edilmesi																		
	1.1.1 Post-kuantum algoritmalı algoritmaların gereksinim analizlerinin yapılması																		
	1.1.2 FIPS 204, FIPS 205 standartları için gerekli algoritmaların alt yapı analizinin yapılması																		
	1.1.3 Post kuantum algoritmalarının mevcut algoritmalar ile birlikte kullanım analiz çalışması																		
	1.2 Ürün araştırması ve analiz edilmesi																		
	1.2.1 Detaylı literatür ve benzer ürün taraması ve takibi																		
	1.2.2 Altyapı kütüphanesinin gereksinimlerinin çıkartılması																		
	1.2.3 Test işlemleri için gerekli koşulların analizinin yapılması																		
	1.3 Gereksinim dokümanının oluşturulması ve tamamlanması																		
	1.3.1 Yazılım Gereksinim Dokümanının isterlere göre oluşturulması ve tamamlanması																		
	1.4 Yönetim dokümanlarının oluşturulması ve tamamlanması																		
	1.4.1 Proje Yönetim Planı, İş Dağılım Ağacı, dokümanlarının oluşturulması ve tamamlanması																		
2. Tasarım					1	2	3	4											
	2.1 Post-Kuantum Algoritmalarının IoT sistemlerine uyumu ile ilgili tasarımlarının çalışılması																		
	2.1.1 SPHINCS+																		
	2.1.2 CRYSTALS-Dilithium																		
	2.1.3 FALCON																		
	2.1.4 Mevcut algoritmalarla birlikte kullanımının tasarlanması																		
	2.2 IoT sistemi içinuygulanacak kodun akışlarının oluşturularak tasarlanması																		
	2.2.1 SPHINCS+ tasarımı																		
	2.2.2 CRYSTALS-Dilithium tasarımı																		
	2.2.3 FALCON tasarımı																		
	2.3 Algoritmalar için test planlarının tasarlanması ve hazırlanması																		
	2.3.1 Algoritma testleri için NIST ve akademik yayınların takibi																		
	2.3.2 Test Planının hazırlanması																		
	2.4 Tasarım Dokümanının oluşturulması ve tamamlanması																		
	2.4.1 Yazılım Tasarım dokümanının (YTD) oluşturulması ve tamamlanması																		
Geliştirme								1	2	3	4	5	6						
	3.1 Post Kuantum Kriptografi Modülü																		
	3.1.1 SPHINCS+ Modülü ile veri şifreleme vs geliştirmesi																		
	3.1.2 CRYSTALS-Dilithium Modülü ile veri şifreleme vs geliştirmesi																		
	3.1.3 FALCON Modülü ile veri şifreleme vs geliştirmesi																		
	3.2 Mevcut Algoritma Modülü																		
	3.2.1 Karar verilen ECC algoritması 1 ile veri şifreleme vs geliştirmesi																		
	3.2.2 Karar verilen ECC algoritması 2 ile veri şifreleme vs geliştirmesi																		
	3.3 Birlikte Kullanım Modülü																		
	3.3.1 Birlikte Kullanım ile veri şifreleme geliştirmesi																		
Entegrasyon												1	2	3					
	4.1 IOT Algoritma Entegrasyonu																		
	4.1.1 PQC entegrasyonu																		
	4.1.2 ECC entegrasyonu																		
	4.1.3 Algoritma birlikte çalışma entegrasyonu																		
	4.2 Entegrasyon Planı Dokümanı																		
	4.2.1 Entegrasyon Planının oluşturulması ve tamamlanması																		
Test													1	2	3				
	4.1 Algoritma işlem testleri																		
	4.1.1 SPHINCS+ işlem doğruluk testleri																		
	4.1.2 CRYSTALS-Dilithium işlem doğruluk testleri																		
	4.1.3 CRYSTALS-KYBER işlem doğruluk testleri																		
	4.1.4 ECC işlem doğruluk testleri																		
	4.2 Hız dayalı performans testleri																		
	4.3 Monte Carlo testleri																		
	4.4 Proje Kapanışının Hazırlığı																		
	4.4.1 Proje çıktılarından elde edilen metriklerin karşılaştırma raporu																		
	4.4.2 Proje Kapanış Raporunun Hazırlanması																		

5. Beklenen Sonuçlar

Proje de beklenen hedefler;

- PQC algoritmalarının verimli olarak IoT sistemlerinde kullanılabilirliğinin gözlemlenmesi,
- PQC algoritmalarının gerekirse mevcut algoritmalarla iç içe birlikte kullanılabilmesinin izlenmesi,
- Kullanılan yeni nesil algoritmaların mevcut algoritmalarda aynı işlemlerde hızlarının yakın olması (~ 2 saniye fark kabul edilebilir olarak belirlenmiştir),
- Kullanılan yeni nesil algoritmaların mevcut algoritmaların güç tüketiminin makul seviyelerinde olması (~ 1.5 katını aşmaması beklenmektedir),

6. Proje Bütçesi

Detaylı bütçe bilgisi ek olarak verilen "Onur_İŞLER_SAHA_Bütçe Formu" adlı maliyet formunda belirtilmiştir.

Genel proje maliyeti:

- Toplam personel maliyeti : 11.650.000 TL
- Donanım maliyeti : 14 USD
- Akadamik Danışman maliyeti: 840.000 TL

7. Riskler ve Önlemler

Tablo 1. Risk ve Önlemler

Risk	***Alınan Önlem***	***Olasılık***	***Etki***	***Alınan Önleme Rağmen Riskin Gerçekleşmesi Durumunda Yapılacaklar***
Algoritmalardan bazılarına kriptografik atak gerçekleşmesi ve kullanılamaz olması	Latis ve Hash tabanlı olmak üzere iki farklı aileden kriptografik algoritmalar bu proje kapsamında kullanılmak üzere belirlenmiştir. Bir aileye yapılacak atak olması durumunda diğer aile ile devam edilecektir.	Düşük	Yüksek	Akademik destek alarak bilimsel gelişmeler yakından takip edilecektir ve atak olan kriptografik algoritmalarla ilgili güncellemeler ivedilikle uygulanacaktır.
STM32 gibi mikrodenetleyicilerin PQC hesaplamalarında zorlanması	Donanımsal hızlandırma veya FPGA gibi alternatif çözümler değerlendirilecek	Orta	Orta	Daha yüksek işlem güvüne sahip mikrodenetleyici araştırması yapılacak, ilgili firmalarla ön görüşmeler yapılacaktır.
Post-quantum algoritmalarının IoT cihazlarında yüksek	Hafifletilmiş PQC algoritmaları ve optimizasyon teknikleri kullanılacak.	Orta	Yüksek	Akademik destek alınarak optimizasyon denenecek ve gerekirse işlemci ailesi değiştirielecek.

işlem yükü yaratması				

8. Proje Süresi

Proje 30.06.2025 ile 31.08.2026 tarihleri arasında toplam süre14 ay olacağı öngörülmüştür. Detaylı bilgi iş zaman grafiğini ve paketleri içeren ek olarak verilen "Onur_İŞLER SAHA proje önerisi iş takvimi.xlsx" adlı dokümanda mevcuttur.

9. Kaynaklar

Bütçe finansmanı için AB proje çağrı başvuruları ve TÜBİTAK tarafından yayınlanan kritik teknolojiler ile ilgili çağrılar takip edilecektir.

Ayrıca NATO DIANA ve NIF Fonları çağrılarında başvuru yapılacaktır.

Bu sebeple Avrupa Birliği programları;

- Horizon Europe (Türkiye tam üye, TÜBİTAK üzerinden Ufuk Avrupa çağrıları),
- EUREKA (Türkiye tam üye, TÜBİTAK üzerinden),
- Digital Europe Programme (Türkiye kısmi çağrılara katılabilir, TÜBİTAK ve BTK bilgilendirme yoluyla çağrı açıyor.)

TÜBİTAK tarafından yayınlanan Ar-Ge ve Yenilik Konu Başlıkları duyurusuna istinaden aşağıdaki programlar;

- 1501 Sanayi Ar-Ge Projeleri Destekleme Programı
- 1507 TÜBİTAK KOBİ Ar-Ge Başlangıç Destek Programı
- 1505 Üniversite-Sanayi İşbirliği Destek Programı (Bu kapsamda üniversite-sanayi iş birlikteliği ile programa başvurulabilir.)
- 1001 Bilimsel ve Teknolojik Araştırma Projelerini Destekleme Programı (Bu kapsamda proje üniversite ve akademisyenler üzerinden hayata geçirilebilir.)

Takip edilecek ve AB programları başvuru sayfaları düzenli takip edilerek olası konsorsiyumlar araştırılacaktır.

10. Değerlendirme Kriterleri

Projenin yöntemi ve çalışma planında bahsedildiği üzere projede kullanılan algoritmaların doğruluğu hazırlanacak veri setleri ile kontrol edilecektir. Ayrıca NIST tarafından

standartlaştırılan test vektörleri ile de doğruluk testleri kontrol edilecektir. Bu sebeple NIST doğruluk testlerinde %90 başarı sağlanması ile proje başarılı kabul edilecektir. Geçemeyen kısımların iyileştirmeleri bakım fazında planlanacaktır.

11. Sonuç ve Beklenen Katkılar

Bu çalışmada gerçekleştirilecek testler ve analizler sonucunda elde edilecek veriler, hem akademik hem de uygulamalı birçok alanda kullanılabilir nitelikte olacaktır. IoT cihazlarında kullanılan mevcut ECC tabanlı güvenlik çözümlerinin performansları ile post-quantum kriptografi (PQC) algoritmalarının (Kyber, Dilithium, SPHINCS+) uygulanabilirliğine dair elde edilecek karşılaştırmalı sonuçlar, özellikle şu alanlara katkı sağlayacaktır:

a. IoT cihaz geliştiricileri için güvenli ve uygun kriptografik algoritmaların seçilmesi sürecine teknik rehberlik sunacaktır.

b. Savunma sanayiinde, akıllı sistemler ve gömülü güvenlik uygulamalarında kuantum sonrası döneme uygun alternatifler oluşturulmasına katkıda bulunacaktır.

c. STM32 gibi mikrodenetleyici platformlarına yönelik optimizasyon sonuçları, gömülü yazılım ve donanım geliştiricileri için kaynak tüketimi ve işlem süresi açısından yol gösterici olacaktır.

d. Lisansüstü tezler ve akademik yayınlar için özgün bir deneysel veri seti sunarak bilimsel bilgi üretimine katkı sağlayacaktır.

e. Kriptografi eğitimi ve laboratuvar çalışmaları için örnek senaryolar ve test ortamları hazırlanmasına altyapı oluşturacaktır.

12. Kaynakça

Onur İŞLER, 2024, “Implementation and Performance Evaluation of Elliptic Curve Cryptography over SECP256R1 on STM32 Microprocessor”, Cryptology ePrint Archive, Paper 2024/1121 (https://ia.cr/2024/1121)

Panos Kampanakis, Peter Panburana, Ellie Daw and Daniel Van Geesı, 2018, “The Viability of PostQuantum X.509 Certificates”

Sikeridis, Dimitrios, Panos Kampanakis, and Michael Devetsikiotis, 2020, “Post-quantum authentication in TLS 1.3: a performance study”

CRYSTALS Team, 2024, https://pq-crystals.org/dilithium/resources.shtml

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang, 2024, https://falcon-sign.info/

SPHINCS+ Team, 2024, https://sphincs.org/resources.htm

NIST FIPS 186-5 Digital Signature Standard (DSS) (2023)