Quantum Computing and the Future of Cyber Security

Project Report - SIB5100 Information Security and Management

1st PhD Student Önder GÖRMEZ
Computer Engineering
Faculty of Electrical and Electronics
Yıldız Technical University
İstanbul, Türkiye
ondergormez@gmail.com

2th Doç. Dr. Özgü CAN
Computer Engineering
Faculty of Engineering
Ege University
İzmir, Türkiye
ozgu.can@ege.edu.tr

***Abstract*—Bu makalede quantum computing teriminin ne olduğu, siber güvenlikle ilişkisi ve post quantum çağında ortaya çıkacak olan güvenlik sorunlarına çözüm olarak üretilmiş olan temel kriptolojik algoritmalar hakkında bilgi verilecektir.**

***Index Terms*—Quantum Computing, Post Quantum Cryptography, Hash-based Signatures, Lattice-based Cryptography, Code-based Cryptography**

I. Introduction

Bu makalede aşağıda listesi verilen konularla alakalı literatür taraması yapılmış ve elde edilen bulgular paylaşılmıştır.

- What is Quantum Computing?
- Post-quantum Cryptography: Hash-based Signatures
- Post-quantum Cryptography: Lattice-based Cryptography
- Post-quantum Cryptography: Code-based Cryptography

II. bölümde quantum computing hakkında kısa bilgiler verilecek, III. bölümde quantum bilgisayarların gelişmesiyle ortaya çıkacak olan güvenlik zaafiyetleri ve risk azaltma tekniklerinden bahsedilecek, IV. bölümde genel olarak kuantum sonrası kriptografinin nasıl olacağı, V. bölümde hash tabanlı dijital imzalar, VI. bölümde lattice tabanlı kriptoloji algoritmaları, VII. bölümde ise kod tabanlı kriptoloji algoritmaları anlatılacaktır. Ve son olarak VIII. bölümde okunan makalelerden çıkarılan sonuçlar ve gelecek çalışmalardan bahesidilecektir.

II. Quantum Computing Hakkında Kisa Bilgiler

A. Kullanılan Terimler Listesi

Kullanılan kısaltmalar ve açılımları Table I üzerinde verilmiştir.

Kuantum ile ilgili literatürde bulunan ve makaleye konu olan kelimelerin listesi ve türkçe karşılıkları Table II üzerinde verilmiştir.

Kısaltma	Açılımı
PQC	Post-Quantum Cryptography
HSM	Hardware Security Module
KMS	Key Management System
XMSS	Extended Merkle Signature System
LMS	Leighton-Micali Signatures
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism Standard
ML-DSA	Module-Lattice-Based Digital Signature Standard
SLH-DSA	Stateless Hash-Based Digital Signature Standard
NIST	National Institute of Standards and Technology
FIPS	Federal Information Processing Standards

TABLE I
Kullanılan Kisaltmalar Listesi

İngilizce Terim	Türkçe Karşılığı
Entangled quantum objects	Dolanık kuantum nesneleri
Quantum bits	Kuantum bitleri
Qubits	Kübitler
Superposition	Üst üste binme
Entanglement	Dolanıklık
Vulnerable Algorithms	Güvenlik Açığı Bulunan Algoritmalar

TABLE II
Kullanılan Terimler Listesi

B. Quantum Computer Nedir?

1981 yılında Richard Feynman karmaşık sistemlerdeki kuantum etkileşimlerini modellemenin yeni bir yolunu önerdi. Bu öneri ilgilendiğimiz fiziksel nesneyi modellemek için dolanık kuantum nesneleri (entangled quantum objects) kullanan bir bilgisayar inşa edilmesiydi. [1]

1981 yılından bu yana kuantum bilgisayarlar hakkında çalışmalar devam etmiştir. Bu çalışmaların başını IBM ve Google gibi büyük firmalar çekmektedir. Hatta IBM yakın zamanda IBM Q System One adında bir ürün çıkararak gelecekteki kuantum bilgisayarların nasıl olacağı hakkında bize bir öngörü sağlamıştır. Fig. 1 ve Fig. 2'de IBM Q System One görülmektedir.

C. Qubit Nedir?

Kuantum bilgisayarının arkasındaki fikir, klasik bitlerimizi kübitler ile değiştirmektir. Klasik bitler 0 veya 1 olabilirken, bir kübit aynı anda 1 veya 0 olma olasılığına sahiptir ve genellikle üç boyutlu uzayda bir birim vektörle gösterilir. [1]

Kuantum hesaplamada kuantum bitleri (quantum bits) veya diğer bir tabirle kübitler (qubits) kullanılır. Üst üste binme

Fig. 1. IBM Q System One İç Yapısı

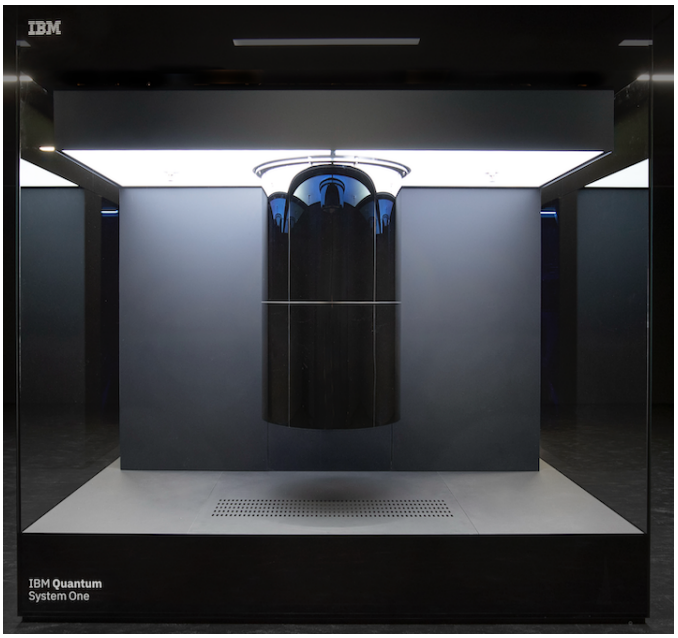

Fig. 2. IBM Q System One Dış Görünüş

(superposition) ve dolanıklık (entanglement) prensipleri nedeniyle, kübitler aynı anda 0, 1 veya her ikisini de temsil edebilir. Fig. 3 de klasik hesaplamada ve kuantum hesaplamada bulunan bit temsilleri gösterilmektedir. [5]

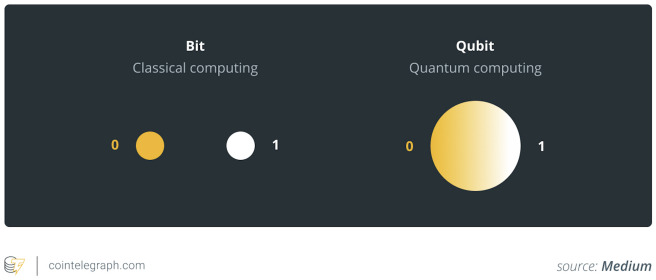

Fig. 3. Classic computing vs quantum computing [5]

III. Quantum Computing ve Siber Güvenlik Riskleri

A. Mosca's Theorem

Waterloo Üniversitesi'ndeki quantum computing araştırmacısı Michael Mosca tarafınfan ortaya atılmış bir teoremdir. Fig. 4 de teoremin denklemi görülmektedir. Teoreme göre;

- x: Secret Key'lerin gizli tutulması gereken süre
- y: Quatum resistance bir algoritmaya geçmek için gereken migration süresi
- z: Quantum bilgisayarların mevcut algoritmayı çözme ve kırma süresi süresi

$x+y > z$ ise kuantum bilgisayarlar gizli anahtarın kullanım süresi dolmadan algoritmayı kırabilir ve sistem hacklenebilir demektir.

Secret Key'i saklamanız gereken süre (x) genellikle uygulamaya göre değişiklik gösterir. Örneğin kredi kartınız için bu süre, kartınızın son kullanma tarihine bağlı olarak iki veya üç yıl olabilir. [1]

Yeni algoritmaya taşınma süresi (y), standardın yazılmaya başlamasından başlar, algoritmanın standartlaşması ve sonrasında kullanıma alınmasına ve ilgili uygulamaya deploy edilmesine kadar geçen süredir. Genel olarak onlarca yıl alabilir şeklinde söyleyebiliriz. [1]

Algoritmanın quantum bilgisayar ile kırılabilmesi için geçmesi gereken süre (z) değeri ise şu anda tamamen bilinmezdir. Bu değişken quantum bilgisayarların başarısının artması ile değeri düşecek bir değişkendir. Michael Mosca'ya göre, 2048-bit RSA algoritması 1/6 ihtimalle 2027 yılında, %50 ihtimalle 2031 yılında savunmasız (vulnerable) kalacaktır ve quantum bilgisayarlar tarafından hızlı bir şekilde kırılabilecektir. [1]

IV. Post Quantum Cryptography

Quantum computing denilince ilk akla gelen konulardan biride kriptoloji alanı ve mevcut kripto algoritmalarının quantum sonrası kullanım durumudur. Literatürde yapılan çalışmalara bakıldığında günümüzde kullandığımız

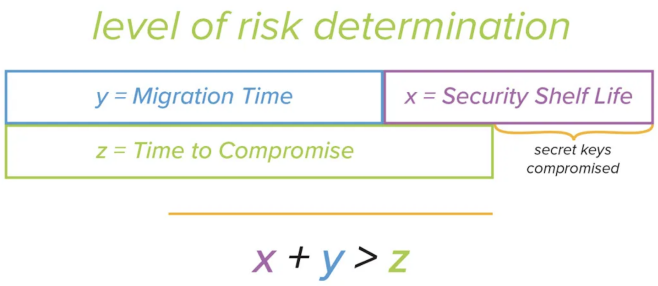

Fig. 4. Mosca's Theorem [1]

çoğu algoritmanın quantum sonrasında kullanılamayacağı öngörülmektedir. Şu anda ne kadar kısa sürede gerçekleşeceği belli olmasa da kullanımdan kalkması gerekecek algoritmalar aşağı yukarı bellidir.

Bu nedenle mevcut sistemlerimizde bu algoritmaların varlığı ve kullanıldığı yerler düzgünce kayıt altına alınmalı, raplacement için uygun vakit geldiğinde hemen değiştirebilmek için aksiyon planı oluşturulmalıdır. Aksiyon planı aşağıdakine benzer olmalıdır. [1]

- RSA, DSA, ECC, DH – gibi çok temel kripto algoritmalarında güvenlik açığı oluşacağının bilincinde olunmalıdır.
- Yukarıda listesi verilen algoritmaları temel alarak kurulmuş TLS, SSH, S/MIME, PGP , IPSEC gibi protokollerin savunmasız kalacağı bilinmelidir.
- VPNs, Kerberos gibi protokollerde yukarıdaki temel algoritmalar ile kurulmuş olan versiyonları bulunabilir.
- Browser lar, encrypted messaging, disk encryption, authentication schemes gibi uygulamalarda yukarıdaki temel algoritmaları kullanıyor olabilirler.

V. PQC: Hash-based signatures

Quantum öncesi imzalama algoritmaları aşağıdaki şekilde çalışır.

- Public/Private Key çifti üretilir. Bu iki key birbiri ile asal sayı ilişkisi içerisindedir.
- Private keyin sahibi sahipliğini kanıtlamak için private key ile veriyi imzalar.
- İmzalanmış veri üzerinde public key ile imza doğrulama işlemi yapılır. Böylelikle datanın private key in sahibinden mi geldiği anlaşılabilmiş olur.

Quantum sonrası imzalama işlemleri için yeni ortaya atılan yöntem ise hash tabanlı imzalama yöntemidir. Bunun tercih edilmesinin en önemli sebebi hash fonksiyonlarının irreversible yani geri döndürülemez olmasıdır.

Fig. 5 de hash tabanlı Public/Private Key Pair oluşturulma süreci gösterilmektedir. Burada random olarak private key seçilir. Public key ise private key in hash i olarak seçilir. Dikkat edilmesi gereken hokta ise her imzalanacak sayı için farklı bir private key üretme gerekliliğidir. Bunun için merkle tree gibi yöntemlerden yararlanılmaktadır.

Hash base imzalama yöntemleri ile alakalı temel konular aşağıda liste olarak verilmiştir.

Value to sign	Private key	Public key
0	sk0 (randomly generate)	pk0(=HASH(sk0))
1	sk1 (randomly generate)	pk1(=HASH(sk1))
2	sk2 (randomly generate)	pk2(=HASH(sk2))
3	sk3 (randomly generate)	pk3(=HASH(sk3))

Fig. 5. Public/Private Key Pair Generation [2]

- Lamport signatures
- Winternitz
- Merkle trees
- Extended Merkle Signature System(XMSS) and Leighton-Micali Signatures (LMS)
- Multi Merkle trees
- Stateful hash-based signatures
- Stateless hash-based signatures

NIST tarafından quantum sonrası çağda kullanılmak üzere kabul edilen SPHINCS+ stateless hash-based bir imzalama algoritmasıdır. [2]

NIST'in web sitesinde [7] finalize edilen 3 algoritmanın 1'i (FIPS 205) hash-based signature algoritmasıdır.

VI. PQC: Lattice-based cryptography

Lattice-based kriptografide vektörler üzerinden hesaplamalar yapılarak kriptolojik işlemler gerçekleştirilir. ECC kriptografideki eliptik eğri denkleminin eğri üzerinde sonsuz tane noktada kesişebilmesi gibi lattice de de sonsuz tane vektör çizilebilir. Fig. 6 de lattice vektörleri görülmektedir.

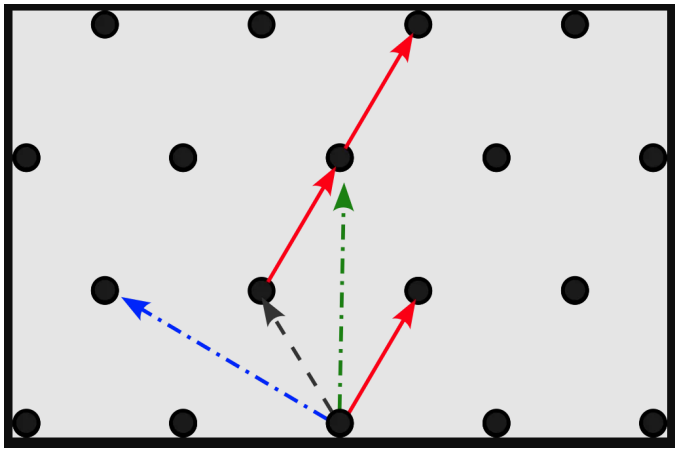

Fig. 6. Vector Lattice-based Cryptography [3]

NIST'in web sitesinde [7] finalize edilen 3 algoritmanın 2'si (FIPS 203, FIPS 204) Lattice based kriptoloji algoritmasıdır.

VII. PQC: Code-based cryptography

Lattice-based algoritmalarda güvenlik açığı oluşacak olursa kullanılabileceği belirtilen code-based kriptografi yöntemidir. Backup senaryosu olarak bu algoritmayı kullanmayı hedeflemişler.

Harberleşme altyapılarında kullanılan error correction code tabanlı bir yönteme dayanmaktadır.

- Hamming Codes

- Goppa Codes

gibi farklı distance yöntemleriyle çalışmalar yapılmıştır.

VIII. Gelecek Çalışmalar

Bu makalede özet olarak quantum computing in geleceği ve siber güvenliğe etkileri temel anlamda incelenmeye çalışılmıştır.

Konu ile alakalı gelecek çalışmalarda aşağıdaki başlıklar incelenebilir.

- Zaman kısıtı nedeniyle makaleye araştırılan teknik detayların hepsi eklenemedi. Referanslar bölümünde yer alan sayfalarda detaylar mevcut. Daha fazla detay için sayfalar incelenebilir.
- Code-based cryptography ile ilgil çalışmalar detaylandırılabilir.
- NIST'in yayınladığı ve sitesinde [7] linki bulunan FIPS 203, FIPS 204, FIPS 205 , FIPS 206 (draft) standartlar incelenebilir.
- NIST'in yayınladığı "Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions" standardı detaylı olarak incelenebilir. [6]

Acknowledgment

Bu makalenin oluşturulmasında ve yayına hazır hale getirilmesinde bizi teşvik eden, geri bildirimlerini ve desteklerini esirgemeyen sayın hocamız Doç. Dr. Özgü CAN'a teşekkürü bir borç bilirim.

References

[1] "Post-quantum cryptography: An introduction" https://www.redhat.com [Online]. Available: https://www.redhat.com/en/blog/post-quantum-cryptography-introduction. [Accessed: 4-Jan-2025].

[2] "Post-quantum cryptography: Hash-based signatures" https://www.redhat.com [Online]. Available: https://www.redhat.com/en/blog/post-quantum-cryptography-hash-based-signatures. [Accessed: 4-Jan-2025].

[3] "Post-quantum cryptography: Lattice-based cryptography" https://www.redhat.com [Online]. Available: https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography. [Accessed: 4-Jan-2025].

[4] "Post-quantum cryptography: Code-based cryptography" https://www.redhat.com [Online]. Available: https://www.redhat.com/en/blog/post-quantum-cryptography-code-based-cryptography. [Accessed: 4-Jan-2025].

[5] "An overview of post-quantum threats to proof-of-work cryptocurrencies" https://cointelegraph.com [Online]. Available: https://cointelegraph.com/learn/articles/post-quantum-threats-to-proof-of-work-cryptocurrencies. [Accessed: 4-Jan-2025].

[6] "Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions" https://www.nist.gov [Online]. Available: https://csrc.nist.gov/pubs/sp/800/232/ipd. [Accessed: 4-Jan-2025].

[7] "NIST Releases First 3 Finalized Post-Quantum Encryption Standards" https://www.nist.gov [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. [Accessed: 4-Jan-2025].