Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

GU J Sci, Part C, 13(3): 892-905 (2025)

Strengthened Key Method in Transition to Quantum Cryptology

Fatih SELVİ[1*] Mustafa ALKAN[2]

[1]*Gazi University, Faculty of Technology, Department of Electrical and Electronics Engineering, Ankara, Turkey*

[2]*Gazi University, Faculty of Technology, Department of Electrical and Electronics Engineering, Ankara, Turkey*

Article Info

Research article
Received: 24/04/2025
Revision: 05/06/2025
Accepted: 23/06/2025

Keywords

Quantum Computers
Post-Quantum Cryptography
Hybrid Encryption
Pre-Shared Key

Makale Bilgisi

Araştırma makalesi
Başvuru: 24/04/2025
Düzeltme: 05/06/2025
Kabul: 23/06/2025

Anahtar Kelimeler

Kuantum Bilgisayarlar
Kuantum Sonrası Kriptografi
Hibrit Şifreleme
Önceden Paylaşılan Anahtar

Graphical/Tabular Abstract (Grafik Özet)

In this study, the effects of quantum computers on classical encryption methods were evaluated and a hybrid encryption method that increases the security of asymmetric encryption algorithms using pre-shared symmetric key (PSK) was proposed. / Bu çalışmada, kuantum bilgisayarların klasik şifreleme yöntemlerine etkileri değerlendirilmiş ve önceden paylaşılan simetrik anahtar (PSK) kullanılarak asimetrik şifreleme algoritmalarının güvenliğini artıran bir hibrit şifreleme yöntemi önerilmiştir.

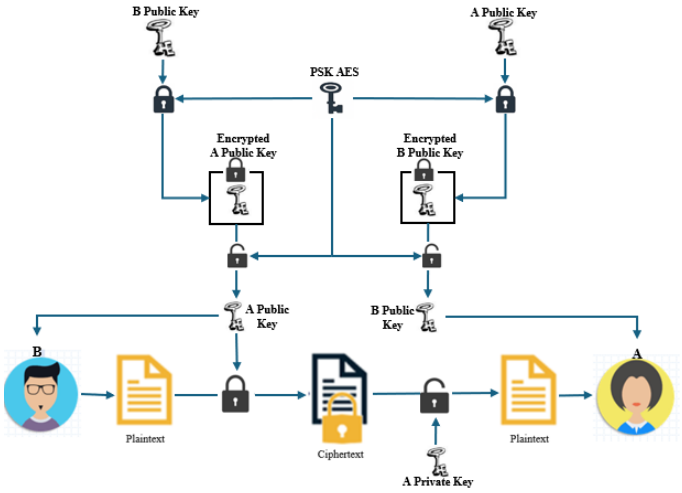

***Figure A**: System Architecture of the Proposed Method / **Şekil A:** Önerilen Yöntemin Sistem Mimarisi*

***Highlights (Önemli noktalar)** The effects of quantum computers on classical cryptographic algorithms have been studied in detail. / Kuantum bilgisayarların klasik kriptografik algoritmalar üzerindeki etkileri detaylı olarak incelenmiştir.*

- *A hybrid encryption method supported by PSK (pre-shared key) has been proposed. / PSK (önceden paylaşılan anahtar) ile desteklenen hibrit bir şifreleme yöntemi önerilmiştir.*
- *The proposed hybrid model provides an additional layer of security during the transition process until the applicability of post-quantum algorithms is ensured. / Önerilen hibrit model, geçiş sürecinde kuantum sonrası algoritmaların uygulanabilirliği sağlanana kadar ek bir güvenlik katmanı sunmaktadır.*

***Aim (Amaç):** Developing a PSK-supported hybrid encryption method to protect data security during the transition period against threats posed by quantum computers. / Kuantum bilgisayarların oluşturduğu tehditlere karşı geçiş sürecinde veri güvenliğini korumak için PSK destekli hibrit bir şifreleme yöntemi geliştirmek.*

***Originality (Özgünlük):** The study proposes a PSK-based hybrid structure that strengthens classical asymmetric encryption methods against quantum attacks and can be integrated into existing systems. / Çalışma, klasik asimetrik şifreleme yöntemlerini kuantum saldırılarına karşı güçlendiren ve mevcut sistemlere entegre edilebilen PSK tabanlı hibrit bir yapı önermektedir.*

***Results (Bulgular):** The proposed hybrid structure provides higher resistance against Shor and Grover algorithms compared to classical systems. / Önerilen hibrit yapı, Shor ve Grover algoritmalarına karşı klasik sistemlere kıyasla daha yüksek dayanıklılık sağlamaktadır.*

***Conclusion (Sonuç):** The proposed PSK-supported hybrid encryption method provides an effective and feasible interim solution to protect data security during the evolution of quantum computers. / Önerilen PSK destekli hibrit şifreleme yöntemi, kuantum bilgisayarların gelişimi sırasında veri güvenliğini korumak için etkili ve uygulanabilir bir ara çözüm sunmaktadır.*

*Corresponding author, e-mail: fatih.selvi@gazi.edu.tr
DOI: 10.29109/gujsc.1682989

GU J Sci, Part C, 13(3): 892-905 (2025)

Gazi Üniversitesi
Fen Bilimleri Dergisi
PART C: TASARIM VE TEKNOLOJİ

Gazi University
Journal of Science
PART C: DESIGN AND TECHNOLOGY

http://dergipark.gov.tr/gujsc

Strengthened Key Method in Transition to Quantum Cryptology

Fatih SELVİ[1*] Mustafa ALKAN[2]

[1]*Gazi University, Faculty of Technology, Department of Electrical and Electronics Engineering, Ankara, Turkey*

[2]*Gazi University, Faculty of Technology, Department of Electrical and Electronics Engineering, Ankara, Turkey*

Article Info

Research article
Received: 24/04/2025
Revision: 05/06/2025
Accepted: 23/06/2025

Keywords

Quantum Computers
Post-Quantum Cryptography
Hybrid Encryption
Pre-Shared Key

Abstract

This study aims to increase security during the transition period against the threats posed by quantum computers to existing cryptographic systems. Since it will take time for post-quantum cryptography standards to become fully applicable, especially asymmetric encryption methods face serious security risks. In this context, a hybrid encryption method that is more resistant to quantum computer attacks is proposed in the study.

The proposed method aims to increase the security of asymmetric algorithms by using pre-shared symmetric key (PSK). In this approach, key distribution is made secure by using symmetric encryption algorithms resistant to quantum attacks such as AES-256. Thus, existing systems gain temporary protection against quantum threats and the transition process is managed more securely.

This study examines the integration of symmetric and asymmetric encryption methods, evaluating the performance and potential security risks of the hybrid approach. It is aimed that the proposed method will contribute to the modernization of national and international cryptographic infrastructure and provide a critical Intermediate solution in the transition process to the post-quantum era.

Kuantum Kriptolojiye Geçişte Güçlendirilmiş Anahtar Yöntemi

Makale Bilgisi

Araştırma makalesi
Başvuru: 24/04/2025
Düzeltme: 05/06/2025
Kabul: 23/06/2025

Anahtar Kelimeler

Kuantum Bilgisayarlar
Kuantum Sonrası Kriptografi
Hibrit Şifreleme
Önceden Paylaşılan Anahtar

Öz

Bu çalışma, kuantum bilgisayarlarının mevcut kriptografik sistemlere yönelik oluşturduğu tehditlere karşı geçiş döneminde güvenliği artırmayı amaçlamaktadır. Kuantum sonrası kriptografi standartlarının tam olarak uygulanabilir hale gelmesi zaman alacağından, özellikle asimetrik şifreleme yöntemleri ciddi güvenlik riskleriyle karşı karşıyadır. Bu bağlamda, çalışmada, kuantum bilgisayarlarının saldırılarına karşı daha dayanıklı hale getirilmiş bir hibrit şifreleme yöntemi önerilmektedir.

Önerilen yöntem, önceden paylaşılan simetrik anahtar (Pre Shared Key - PSK) kullanılarak asimetrik algoritmalarının güvenliğini artırmayı hedeflemektedir. Bu yaklaşımda, AES-256 gibi kuantum saldırılarına karşı dirençli simetrik şifreleme algoritmaları kullanılarak anahtar dağıtımı güvenli hale getirilmektedir. Böylece, mevcut sistemler kuantum tehditlerine karşı geçici bir koruma kazanmakta ve geçiş sürecinin daha güvenli bir şekilde yönetilmesi sağlanmaktadır.

Bu çalışma hem simetrik hem de asimetrik şifreleme yöntemlerinin entegrasyonunu ele alarak, hibrit yapının performans analizi ve potansiyel güvenlik risklerini değerlendirmektedir. Önerilen yöntemin, ulusal ve uluslararası kriptografik altyapının modernizasyonuna katkı sağlayarak, kuantum sonrası döneme geçiş sürecinde kritik bir ara çözüm sunması hedeflenmektedir.

1. INTRODUCTION (GİRİŞ)

Quantum computers have the potential to initiate radical change, especially in the field of cryptography, thanks to their computational power that goes beyond classical computers. Traditional asymmetric encryption algorithms can be rendered ineffective in a short time thanks to the advanced capabilities of quantum computers. Quantum algorithms, such as the Shor algorithm, have the capacity to effectively break widely used asymmetric encryption methods, especially RSA, DSA and ECC [1]. This threatens existing digital security protocols, posing serious security risks for critical infrastructures, sensitive data and communication systems.

*Corresponding author, e-mail: fatih.selvi@gazi.edu.tr
DOI: 10.29109/gujsc.1682989

In this context, important work is being carried out to develop and standardize post-quantum cryptographic algorithms. In the process initiated by the National Institute of Standards and Technology (NIST), standards for algorithms resistant to quantum computers have been determined, but it is foreseen that a long transition period will be required for the integration of these algorithms into existing systems [2]. During this transition period, intermediate solutions are needed to secure existing systems and make them resistant to quantum threats.

The transition period refers to the critical period until post-quantum cryptographic algorithms become fully viable. During this period, existing encryption infrastructures face the risk of being vulnerable to quantum computers. In particular, it is imperative to implement practical, applicable and secure solutions during this period, especially for the security of sensitive data. At the same time, both existing systems need to be modernized and made compatible with post-quantum systems in the long term. The costs, technical challenges and integration problems that arise in this process represent a major challenge for both the public and private sectors.

This study aims to present a method for making existing asymmetric encryption algorithms more resistant to quantum computer threats during the transition process. In the proposed approach, symmetric encryption algorithms such as AES-256, which are also evaluated by NIST as being resistant to quantum computers, are used to support asymmetric encryption processes with the pre-shared key symmetric key method [3] [4]. This approach is particularly notable in terms of both its practical applicability and compatibility with existing systems.

The article focuses on the post-quantum transition process and discusses the integration of symmetric and asymmetric encryption techniques, the technical challenges of this integration, and the potential benefits. Thus, it aims to provide a temporary but effective solution to the threats posed by quantum computers.

1.1. Fundamentals of the Research (Araştırmanın Temelleri)

The development of quantum computers threatens classical asymmetric algorithms, especially RSA and ECC, and necessitates the transition to post-quantum cryptography [1]. This study proposes a hybrid encryption structure supported by pre-shared AES-256 symmetric keys in order to provide a solution resistant to quantum attacks during the transition process.

The proposed methodology aims to protect data security until the standardization of post-quantum algorithms and provides a structure that can form the basis for future adaptations.

1.2. Definition of the Existing Problem (Mevcut Sorunun Tanımlanması)

Asymmetric algorithms such as RSA and ECC are based on mathematical foundations that can be solved by quantum computers in a short time with the Shor algorithm. On the other hand, symmetric algorithms such as AES are more robust despite the Grover algorithm; they offer a high level of security, especially with key sizes of AES-256 and above [4].

For this reason, hybrid structures supported by pre-shared symmetric keys stand out as an effective and applicable intermediate solution against quantum attacks during the transition process.

2. LITERATURE REVIEW (LİTERATÜR İNCELEMESİ)

The impact of quantum computers on cryptographic systems has been intensively discussed in recent years, both in academic circles and in industry. The development of the Shor algorithm in 1994 was a significant turning point in the fact that asymmetric encryption algorithms could be effectively broken with quantum computers [1]. This development called into question the long-term security of common asymmetric algorithms such as RSA, ECC and DSA.

Symmetric encryption algorithms, on the other hand, have been evaluated more resistant to quantum computers. Although Grover's algorithm can effectively halve the encryption key size of symmetric algorithms, algorithms with longer key sizes such as AES-256 have been shown to be resistant to quantum threats [4]. Therefore, symmetric algorithms are considered to provide a durable foundation for quantum computers [5].

The studies initiated to develop algorithms resistant to the threats of quantum computers gained momentum with the standardization process of quantum-resistant crypto algorithms announced by NIST in 2016 [2]. As a result of this process, the publication of the first standards in 2024 has been an important step towards long-term solutions against quantum computer threats. However, the integration of these algorithms into existing systems

will take much longer and will require a costly transition period.

In the transition period, solutions are being sought against future-oriented threats, especially with quantum computers such as “harvest then decrypt” [6]. In this context, the idea of increasing the resilience of existing asymmetric systems using symmetric encryption algorithms comes to the fore. In particular, combining the AES-256 key distributed with the pre-shared symmetric key method and asymmetric encryption methods has the potential to provide effective intermediate solutions against quantum threats [7].

In recent years, intensive studies have been conducted in the literature on the feasibility, performance and cost impacts of these intermediate solutions. Studies show that the quantum transition process is considered a critical challenge both at the academic and industrial levels. This literature review examines in detail the current status of applicable intermediate solutions and the technical challenges that need to be solved in the transition period to quantum cryptography.

3. CLASSICAL CRYPTO METHODS (KLASİK KRİPTO YÖNTEMLERİ)

3.1. Symmetric Encryption Methods (Simetrik Şifreleme Yöntemleri)

Symmetric encryption is an encryption method in which the same secret key is used for encryption and decryption operations. This method is highly effective for encrypting large volumes of data due to its advantages of high speed and low computational cost. The parties involved in communication perform data encryption and decryption operations using a single, pre-shared secret key [8]. The security of the system depends on keeping this key secret. The system architecture of this structure is presented in Figure 1.

Symmetric encryption algorithms are divided into two main categories: block encryption (e.g. DES, AES) and stream encryption (e.g. RC4). Nowadays, block encryption algorithms, especially AES, are more widely preferred due to their high security and performance advantages.

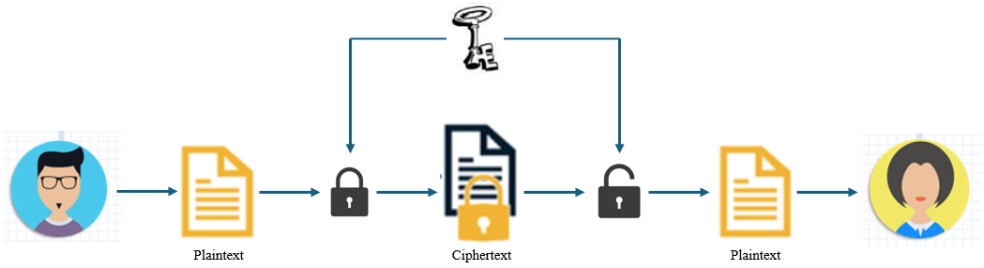

Figure 1. Symmetric Encryption and Decryption (Simetrik Şifreleme ve Şifre Çözme)

Symmetric encryption is preferred especially in applications where performance is at the forefront due to its high speed and low resource consumption [9]. However, the most important limitation of this method is the difficulty of securely sharing the secret key. In addition, key management in multi-user systems can become complex and lead to scalability problems.

3.2. Asymmetric Encryption Methods (Asimetrik Şifreleme Yöntemleri)

Asymmetric encryption is a method where two different, but mathematically related keys (public and private keys) are used for encryption and decryption operations in order to ensure data security [10]. While the public key is known and used by everyone, the private key is stored and used only by authorized persons. This method, whose system architecture is shown in Figure 2., plays an important role in applications such as secure communication, digital signatures and authentication, especially on the Internet. Among the asymmetric encryption methods, RSA (Rivest-Shamir-Adleman), ElGamal and ECC (Elliptic Curve Cryptography) algorithms are among the most widely used and preferred algorithms in security applications [11].

Asymmetric encryption offers significant advantages by overcoming the problem of key sharing and providing authentication. However, it is not suitable for large data sets because it requires higher processing power than symmetric encryption methods. In addition, quantum algorithms such as Shor's algorithm have the potential to break these methods.

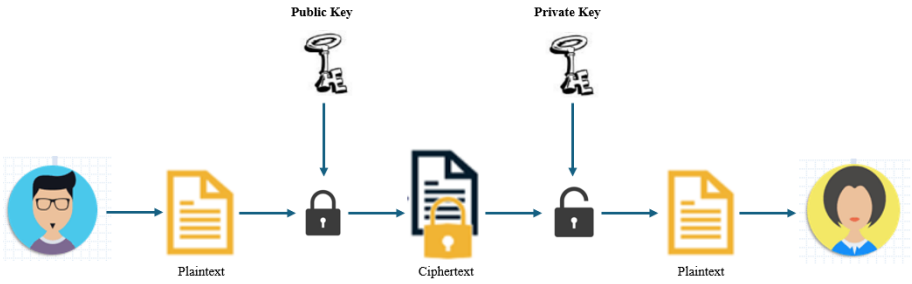

Figure 2. Asymmetric Encryption and Decryption (Asimetrik Şifreleme ve Şifre Çözme)

4. THE IMPACT OF QUANTUM COMPUTERS ON CURRENT ENCRYPTION METHODS (KUANTUM BİLGİSAYARLARININ MEVCUT ŞİFRELEME YÖNTEMLERİNE ETKİSİ)

The development of quantum computers fundamentally threatens the security of traditional cryptographic algorithms [12]. Existing encryption methods based on mathematical problems that are impractical to solve with classical computers are becoming breakable thanks to the high parallel processing power offered by quantum computers. This situation affects both asymmetric and symmetric encryption algorithms at different levels.

Quantum computers use units of information called qubits, which are based on the principles of quantum mechanics, instead of classical bits for information processing. Thanks to their superposition property, qubits can represent multiple states at the same time, giving quantum computers the ability to perform highly parallel computing. Entanglement allows the quantum states of multiple qubits to become interdependent, allowing all components of the system to work together faster and more efficiently.

These features allow quantum computers to work much more efficiently than classical systems on certain mathematical problems. In particular, quantum algorithms such as Shor and Grover have the potential to neutralize asymmetric encryption systems and weaken the security level of symmetric algorithms. Therefore, quantum computers pose a serious threat to existing cryptographic infrastructures.

4.1. Impact of the Shor Algorithm on Existing Encryption Methods (Shor Algoritmasının Mevcut Şifreleme Yöntemlerine Etkisi)

Developed by Peter Shor in 1994, the Shor algorithm is a quantum algorithm that demonstrates the superiority of quantum computers in solving certain mathematical problems that are very difficult for classical computers. The algorithm works especially on prime factorization and modular arithmetic. These features threaten the fundamental security principles of popular asymmetric encryption algorithms such as RSA.

4.1.1. Effect on RSA Encryption (RSA Şifreleme Üzerindeki Etkisi)

The RSA algorithm is based on the difficulty of factoring a number obtained by multiplying two large prime numbers. While on classical computers this process is so difficult that it can take years, thanks to Shor's algorithm, quantum computers can do it in a fraction of the time.

Fundamentals of RSA Encryption System: RSA Encryption is based on the value N obtained by multiplying two large prime numbers p and q. The difficulty of separating this value into prime factors ensures the security of the algorithm [10]. The key space ϕ (N) is calculated with the following Formula 1.

$$\phi(N) = (p - 1)(q - 1) \quad (1)$$

The relationship between the public key e and the private key d in formula 2 is provided

$$e \times d \equiv 1 \pmod{\phi(N)} \quad (2)$$

The Prime Factorization Problem: RSA encryption security relies on the difficulty of not knowing the prime factors p and q that make up N. For classical computers, this problem requires impractical computational time for large values of N. A 2048-bit N can take thousands of years to factorize with classical computers.

4.1.2. Solution Process of Shor Algorithm (Shor Algoritmasının Çözüm Süreci)

The Shor algorithm exploits quantum mechanical properties to find the prime factors of N. This

process consists of the following mathematical steps:

Period Finding Problem: Shor's algorithm reduces the prime factorization problem to a period finding problem [9]. The mathematical basis for this is:

- A random number a is chosen ($1 < a < N$)
- If a and N are prime between them, there is a smallest r (period) satisfying the equation $r \equiv 1 \pmod{N}$.
- With the help of r, the factors of N can be calculated with formula 3:

$$p = \text{ebob}(ar/2 - 1, N), \quad q = \text{ebob}(ar/2 + 1, N) \quad (3)$$

Quantum Fourier Transform: It is difficult to find r with classical methods. Shor's algorithm uses the quantum Fourier transform to find r much faster than classical computers [13].

4.1.3. Conclusion (Sonuç)

The security of the RSA algorithm is based on the difficulty of dividing a number obtained by multiplying two large prime numbers into prime factors. For classical computers, this process becomes exponentially more difficult as the size increases, and it is practically impossible to break. However, quantum computers make the difficult problems that form the basis of asymmetric algorithms such as RSA meaningless thanks to the power of Shor's algorithm.

While todays widely used 2048-bit RSA keys can take thousands of years to broken with classical computers, it is theoretically predicted that a quantum computer with a capacity of 4096 logical qubits could do it in a few hours. It is estimated that approximately 10-20 million physical qubits would be needed to obtain 4096 logical qubits [14]. Today, however, the quantum computers needed to implement the Shor algorithm do not yet have sufficient qubit capacity and error correction mechanisms.

In 2018, researchers used IBM's 5- and 16-qubit quantum processors to prime factorize numbers such as 4,088,459 and 966,887 [15]. In 2022, Chinese researchers reported that they were able to prime factor 48-bit integers using 10 superconducting qubits [16].

4.2. The Effect of Grover Algorithm on Current Encryption Methods (Grover Algoritmasının Mevcut Şifreleme Yöntemlerine Etkisi)

The Grover algorithm is a powerful quantum algorithm that allows quantum computers to be faster than classical computers in solving a certain type of problem [17]. This algorithm provides advantages especially in key search processes used in symmetric encryption methods. Its effect is more limited compared to the Shor algorithm and only accelerates brute-force attacks; therefore, it poses a threat only against symmetric algorithms, not asymmetric ones.

4.2.1. Impact on AES Encryption (AES Şifreleme Üzerindeki Etkisi)

AES (Advanced Encryption Standard) is one of the most widely used strong symmetric encryption algorithms today, offering different key lengths (AES-128, AES-192, AES-256). Its security is based on the fact that it is practically impossible to implement brute force attacks where all possible key combinations are tried. However, the new computational models offered by quantum computers, in particular the Grover algorithm, pose a potential threat by accelerating this search process by a square root.

The AES algorithm consists of SubBytes, ShiftRows, MixColums and AddRoundKey. Each round of these operations increases the randomness and complexity of the data. The number of rounds increases with the key length (10 rounds for AES-128, 12 rounds for AES-192, 14 rounds for AES-256) [8].

4.2.2. Grover Algorithm Solution Process (Grover Algoritmasının Çözüm Süreci)

Grover algorithm can solve the problem in $\sqrt{N}$ steps, the number of N attempts required in classical methods to find the correct key. This works as follows for the AES algorithm [18]:

- AES-128: $2^{128} \rightarrow$ Grover iteration number $\approx 2^{64}$
- AES-256: $2^{256} \rightarrow$ Grover iteration number $\approx 2^{128}$

4.2.3. Quantum Computer Requirements (Kuantum Bilgisayar Gereksinimleri)

In order to effectively implement the Grover algorithm on AES, quantum computers must meet certain technical requirements.

- Number of Logical Qubits: For Grover's algorithm, several thousand logical qubits are

required to represent a 246-bit key size in AES-256 and to run the algorithm.

- Physical Qubit Count: Due to error correction mechanisms, millions of physical qubits are required. For example, in Grassl et al.'s (2015) work, if approximately 6,681 logical qubits are used to break AES-256 and approximately 5,000 physical qubits are used for one logical qubit when error corrections are included, 33,405,000 physical qubits are required [4].

4.2.4. Estimated Processing Time (Tahmini İşlem Süresi)

How many quantum gates a quantum computer can run per second affects the processing time. Estimated processing time for the Grover algorithm:

- AES-256: 2^{128} steps are assumed to be required.
- On a system with 10^9 quantum operations per second, this would be $\approx 3.4\times10^{29}$ seconds [19].

As a result of this calculation, the search time is too long to be realized in practice, indicating that AES-256 is still secure against quantum.

4.2.5. Conclusion (Sonuç)

The AES algorithm is a symmetric encryption algorithm that is widely used and considered secure today. The development of quantum computing, especially with the Grover algorithm, poses some threats to the security of symmetric encryption methods such as AES, but its practical impact is limited.

The Grover algorithm poses a significant threat to the security of AES, but the capacity of existing quantum computers prevents the practical applicability of this attack. In addition, its impact can be significantly limited when the right precautions are taken (for example, switching to AES-256 or AES-512). Despite the theoretical power of quantum computers, the security of symmetric encryption methods is seen to be sustainable for a certain period of time in the quantum age.

As a result, symmetric encryption methods can be protected against the threats of the Grover algorithm by using longer key lengths and updating security standards. However, these threats will require continuous evaluation and adaptation in parallel with the development of quantum computers.

4.3. Comparative Analysis of Encryption Algorithms Against Quantum Computers (Kuantum Bilgisayarlarına Karşı Şifreleme Algoritmalarının Karşılaştırmalı Analizi)

In this section, the resistance of widely used symmetric (AES) and asymmetric (RSA, ECC) encryption algorithms against quantum computers is analyzed comparatively with parameters such as the security basis of the algorithm used, its weaknesses against Grover and Shor algorithms, the number of logical qubits required and the estimated quantum breaking time.

The table below summarizes the post-quantum security levels of both symmetric and asymmetric algorithms and supports the necessity of the proposed hybrid structure with technical justifications.

Table 1. Durability Comparison of Encryption Algorithms Against Quantum Computer (Kuantum Bilgisayara Karşı Şifreleme Algoritmalarının Dayanıklılık Karşılaştırması)

Algorithm	Post-Quantum Security Level	Required Qubit (Logical)	Theoretical Breaking Time	Resistance
RSA-1024	0 bit (Shor)	≈2000	A few minutes	Very low
RSA-2048	0 bit (Shor)	≈4096	A few hours	Very low
ECC-256	0 bit (Shor)	≈2330	A few hours	Very low
AES-128	64 bit (Grover)	≈3000	$\approx1.84\times10^{10}$ Seconds	Medium
AES-256	128 bit (Grover)	≈6681	$\approx3.4\times10^{29}$ Seconds	High
AES-512	256 bit (Grover)	>>10000	$\approx1.16\times10^{60}$ Seconds	Very High
Proposed Model (PSK AES 256 + Asymmetric)	128 bit (Grover)	≈6681	$\approx3.4\times10^{29}$ Seconds	High

The data obtained from the table justifies why the symmetric structure should support the asymmetric structure in the proposed hybrid encryption model. Thus, the security of existing systems can be ensured during the transition to the post-quantum era.

5. TRANSITION PROCESS AND INTERMEDIATE SOLUTIONS (GEÇİŞ SÜRECİ VE ARA ÇÖZÜMLER)

The development of quantum computers is one of the most important technological advances that directly threaten the security of traditional cryptographic systems. Although fully widespread and stable quantum computer systems have not yet been achieved, the potential of these technologies to erode cryptographic infrastructures in the medium term has necessitated a cryptographic transition process [3]. In the transition period until the maturity of post-quantum algorithms, security measures to be taken and temporary solutions to be developed in order to protect existing systems are of strategic importance.

This transition process is not only a transformation at the algorithm level, but also a complex transformation process that requires updating the existing information systems architecture. In particular, hybrid cryptographic approaches stand out as an effective temporary solution in making the existing infrastructure quantum resistant.

5.1. Fundamental Challenges of the Post-Quantum Transition (Kuantum Sonrası Geçişin Temel Zorlukları)

The transition to the post-quantum era brings with it multidimensional challenges at technical, operational, economic and strategic levels. Existing encryption methods used in a wide range of fields, from government institutions to the private sector, are not resilient to quantum computing, requiring a fundamental restructuring of the system.

In addition, the applicability of post-quantum algorithms is still under research and development. In addition to software and hardware upgrades to make the algorithms viable, it also requires hardware compatibility, restructuring of communication protocols, changing data formats and implementing new key management mechanisms [6]. Realizing this transformation requires costly investments as well as multi-layered planning such as corporate strategy, personnel training and legal regulations.

The most critical need in this process is "intermediate solutions" that can provide temporary but effective protection. In this context, hybrid encryption approaches that use both classical and quantum-resistant algorithms together come to the fore. While hybrid systems work in harmony with classical infrastructures, they also provide a certain level of resistance against quantum attacks and allow the transition process to be managed more securely.

5.2. Transition Process (Geçiş Süreci)

Adapting existing crypto infrastructures to quantum-secure algorithms is a complex process. It requires not only technological change, but also a large-scale adaptation process. This process includes several important stages, listed below.

5.2.1. Awareness and Risk Assessment (Farkındalık ve Risk Değerlendirmesi)

It is of utmost importance for organizations to understand the potential impact of quantum computing on cryptographic systems and perform detailed risk analyses of their existing infrastructure. While asymmetric algorithms such as RSA can theoretically be broken in a short time with the Shor algorithm, symmetric algorithms such as AES can be weakened by halving the effective key space with the application of the Grover algorithm. Therefore, strategic decisions should be made by evaluating which algorithms can remain secure for how long.

The risk assessment conducted by NIST found that the United States should prioritize the timely transition of asymmetric cryptographic systems to quantum cryptography and aims to reduce quantum risk as much as possible by 2035 [3]. However, it was assessed that transition timelines may vary depending on the specific use case or application, and it was recommended that systems with long-term privacy needs or more complex cryptographic infrastructures may transition to quantum cryptography earlier. In addition, in its assessment of symmetric encryption methods, it was stated that at least 128-bit symmetric encryption algorithms meet the requirement of at least Category 1 security in the five security strength categories system for the evaluation parameters in the NIST post-quantum cryptography standardization process, while the 256-bit symmetric encryption algorithm meets Category 5 security and is resistant to attacks by quantum computers for many years. 112-bit symmetric encryption algorithms will be banned by 2030 [20].

Similarly, in the risk assessment conducted by the German Federal Information Office (BSI), it was emphasized that 128-bit symmetric encryption algorithms could be broken by quantum computers in the coming period and therefore 256-bit symmetric encryption algorithms would be resistant to quantum computers in the long term. Regarding asymmetric encryption algorithms, it was assessed that systems should be transformed in the short term [21].

5.2.2. Adaptation of Existing Systems (Mevcut Sistemlerin Uyarlanması)

Workarounds can be applied until quantum computers are fully operational. Especially the development of hybrid systems is important. Hybrid systems use both classical algorithms and post-quantum cryptographic solutions together, minimizing security vulnerabilities during the transition process.

5.2.3. Updating Standards (Standartların Güncellenmesi)

NIST's setting of post-quantum cryptography standards is a critical step in this process. With the standards published in August 2024, the applicability of quantum secure algorithms has accelerated. However, integrating these algorithms into existing systems will require a long transition period, both technically and operationally. According to NIST's estimates, this process will take between 10 and 20 years [3].

5.3. Intermediate Solutions (Ara Çözümler)

Since it will take time for post-quantum cryptography (PQC) algorithms to become fully applicable, it is critical to develop temporary but effective security solutions during the transition process. In this context, the inter solutions developed will help maintain data security by integrating into existing infrastructures, while also ensuring that the transition to quantum-resistant systems takes place on a more secure basis.

5.3.1. Hybrid Algorithms with PSK (Pre-shared key) Symmetric Encryption Keys (PSK (Önceden paylaşılan anahtar) Simetrik Şifreleme Anahtarları ile Hibrit Algoritmalar)

In line with the prediction that asymmetric algorithms will be vulnerable to quantum computers, hybrid encryption structures supported by pre-shared symmetric keys are proposed. In this approach, symmetric algorithms such as AES, which are relatively more resistant to quantum attacks, are used in combination with asymmetric algorithms that can become vulnerable. In particular, the quantum resistance of AES-256 is emphasized in literature, and PSK-based hybrid structures stand out as an effective intermediate solution in the transition process.

5.3.2. Strengthening Symmetric Encryption Keys (Simetrik Şifreleme Anahtarlarının Güçlendirilmesi)

Although symmetric algorithms are more resistant to quantum attacks than asymmetric systems, it is important to increase the key length due to the effect of the Grover algorithm. In order to mitigate the effect of Grover's algorithm, it is recommended to switch to longer key sizes such as AES-256 or AES-512 [4]. Such a measure provides additional resistance to the parallel computing power offered by quantum computers.

5.4. Application Areas and Strategic Approaches (Uygulama Alanları ve Stratejik Yaklaşımlar)

Intermediate solutions adopted in the transition process have strategic importance in areas requiring high security such as public institutions, the financial sector, healthcare services and the defense industry [22]. Effective planning of these solutions is directly related to their integration into systems and increasing the competence of the relevant personnel.

As a result, the transition process and intermediary solutions play a critical role both in the preparation process for the adoption of post-quantum algorithms and in ensuring the security of existing data. Intermediate solutions developed in this process will not only ensure the protection of the existing infrastructure, but also in preparation for the future post-quantum era. Therefore, studies on the transition process will create a more solid foundation for the post-quantum era, both technically and strategically.

6. PROPOSED METHOD AND METHODOLOGY (ÖNERİLEN YÖNTEM VE METODOLOJİSİ)

The steps of the hybrid encryption protocol designed by encrypting asymmetric parameters with a pre-shared symmetric key are presented below, and the schematic system architecture is shown in Figure 3.

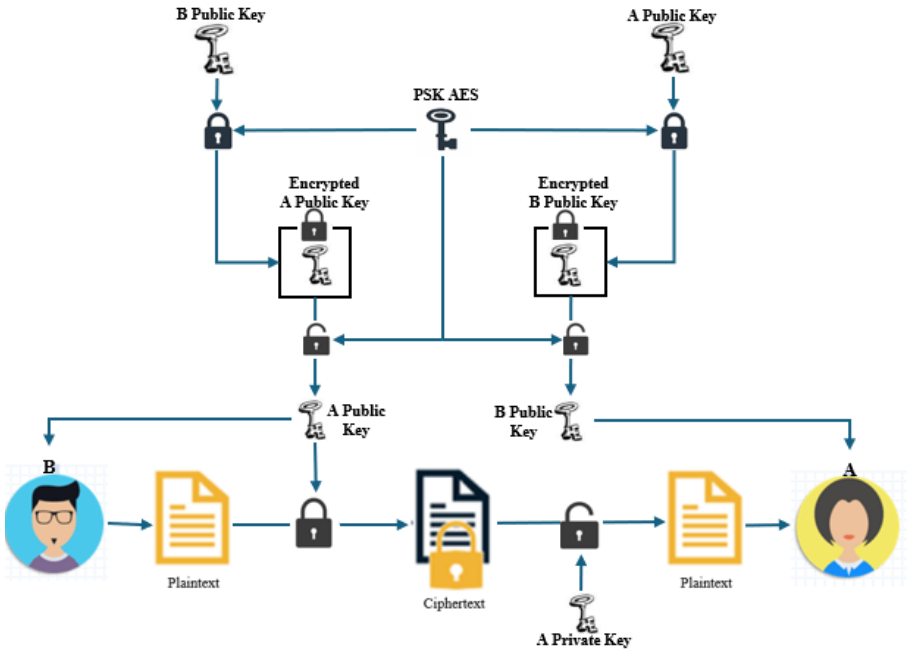

Figure 3. System Architecture of the Proposed Method (Önerilen Yöntemin Sistem Mimarisi)

Key Sharing: The Receiver (A) and the Sender (B) share a common symmetric key (PSK) through a secure channel (e.g. courier, face-to-face meeting). This key is a public and secret key for both parties.

Asymmetric Key Pair Generation: Both parties generate their own public and private key pairs using classical methods.

- A generates its own public (A Public) and private (A Private) key pair.
- B generates its own public (B Public) and private (B Private) key pair.

Asymmetric Key Encryption: The parties encrypt public key with the pre-shared AES-256 key.

- A encrypts public key with AES 256, AES-256 (PSK, A public).
- B encrypts public key with AES 256, AES-256 (PSK, B public).

Sending Encrypted Asymmetric Key: Encrypted public keys are exchanged.

- A sends the encrypted A public key (AES-256 (PSK, A public)) to B.
- B sends the encrypted B public key (AES-256 (PSK, B public)) to A.

Decryption of the Encrypted Asymmetric Key: The parties decrypt the encrypted keys they receive with the pre-shared symmetric key.

- B decrypts the encrypted public key A (AES-256 (PSK, A public)) received from A with PSK.
- A decrypts the encrypted public key B (AES-256 (PSK, B public)) received from B with PSK.

Asymmetric Encryption Process: After the key exchange is completed, the parties can continue secure communication using standard asymmetric encryption protocols.

This hybrid architecture offers additional protection against the threats posed by quantum computers to asymmetric encryption algorithms by using the robustness of symmetric encryption. It is a temporary but effective security measure that can be implemented especially during the transition period, before the post-quantum algorithms are fully standardized. This not only maintains compatibility with existing infrastructure but also provides an enhanced level of data security.

6.1. PSK Distribution, Model Integrity and Key Renewal Approach (PSK Dağıtımı, Model Bütünlüğü ve Anahtar Yenileme Yaklaşımı)

Since the security of the proposed hybrid model is based on the privacy of the symmetric PSK, how this key is distributed and managed is critical.

6.1.1. Safe Distribution of PSK (PSK'nın Güvenli Dağıtımı)

The secure sharing of PSK between the parties is one of the basic security assumptions of the system.

One of the methods of secure sharing is physical distribution such as courier, face-to-face meeting or manual transfer in a secure environment. The other method is to transfer PSK over isolated internal networks that are not connected to the outside world. Such networks can be preferred in terms of secure key transfer since they are closed systems protected from external threats. These options can be selected according to the operational conditions of the system and can be used together with the hybrid cryptography approach.

6.1.2. The Role of PSK in the Proposed Model (Önerilen Modelde PSK'nın Rolü)

In the general structure of the proposed model, PSK is used only for encryption of public keys used at the beginning of communication and acts as a preliminary protection layer of asymmetric encryption. Thanks to this usage, PSK does not carry continuous transmission throughout the entire session, it is only active for initial key sharing. The model follows the following structure:

- PSK is used only to hide public keys
- After the public keys are decrypted, standard asymmetric communication continues.
- PSK does not provide a direct encryption function for the message data.

6.1.3. Key Renewal Approach (Anahtar Yenileme Yaklaşımı)

It is recommended that PSK be renewed periodically to ensure the continuity of system security. In this context;

Renewal of PSK Used in the System According to Frequency of Use: PSK can be renewed daily or hourly depending on the intensity of the system, usage traffic and most importantly the security level. The renewal frequency can increase as the security level increases.

Distribution and Use of PSK According to Time Periods: PSKs are produced and distributed to the parties in 1-month, 3-month or 6-month periods according to secure distribution possibilities. During each distribution period, PSK is renewed and used within the system at certain time intervals (daily or hourly). In order to prevent confusion, these keys are marked with time codes and each key contains a validity period that matches the parties' system clock. In this way, the parties can correctly understand which PSK will be used in which time period. In addition, spare keys are produced and delivered to the parties during key distribution periods in case of a PSK being seized by someone else or suspected.

The process of periodic renewal of PSK is controlled by the central authority of the system or the security manager. This central structure generates new PSKs at specified time intervals and transmits them to the communicating parties through predetermined channels.

6.2. Strengths of Hybrid Encryption Method (Hibrit Şifreleme Yönteminin Güçlü Yanları)

6.2.1. Security (Güvenlik)

Hybrid encryption has been developed to provide a defense against potential threats from quantum computers by increasing the security level of existing encryption systems. In particular, the additional layer of security provided by symmetric encryption keys plays a critical role against the capacity of quantum computers to break existing asymmetric encryption algorithms.

Asymmetric Key Security: In asymmetric encryption algorithms, the public key is usually shared publicly. However, these keys are the weakest part against quantum computer attacks. The hybrid method provides a more resistant structure against attacks by quantum computers by ensuring that public keys are encrypted with a symmetric key.

Use of Secure Channel in Key Distribution: Since the symmetric key is transmitted between the parties through a secure channel (e.g. face-to-face meeting, physical courier, mail), it minimizes security gaps in the key sharing process. This significantly reduces the risk of third parties accessing the key.

Multi-Layered Security: With the double-layered security model offered by the hybrid method, protection is provided with symmetric encryption against the possibility of breaking the asymmetric encryption method. Even if the symmetric key is captured, the asymmetric encryption method needs to be broken in order to decrypt the system.

6.2.2. Adaptability (Uyarlanabilirlik)

It will take 10-20 years for quantum-resistant algorithms to become fully applicable, and this process will require modernization or replacement of existing infrastructures [3]. This poses a great challenge in terms of time and cost. Hybrid encryption method is compatible with existing encryption systems, allowing systems to transition to quantum security quickly and cost-effectively.

Use of Existing Infrastructure: Hybrid encryption does not require fundamental changes to the existing asymmetric encryption infrastructure. Common algorithms such as RSA and ECC are converted into a hybrid structure by integrating only symmetric keys. This approach increases the security of the existing infrastructure while eliminating costly infrastructure changes. Furthermore, hybrid methods continue to secure existing cryptosystems before quantum-resilient algorithms are implemented during the transition.

Integration: Integration of hybrid encryption method is a relatively simple process in terms of software and hardware. This increases the applicability in a wide range from small-scale systems to large networks.

6.2.3. Quantum Resistance (Kuantum Dayanıklılığı)

The hybrid encryption method offers a strong defense mechanism against the potential of quantum computers to break existing asymmetric encryption algorithms.

Resistance of Symmetric Encryption: Symmetric encryption algorithms (e.g. AES-256) are more resistant to quantum computers' methods, such as the Grover algorithm. Although Grover's algorithm reduces symmetric encryption to half the security level of classical encryption, a strong algorithm like AES-256 still provides a security level of 128 bits. In the event of the development of quantum computers, the level of security can be further increased by switching to stronger encryption methods such as AES-512 [19]. In addition, encrypting asymmetric encryption keys with symmetric keys provides additional security, as the attacker must break not only the asymmetric algorithm but also the symmetric key.

Preparation for the Post-Quantum Era: If quantum computers are fully developed and widespread, hybrid systems based on the strength of the symmetric encryption key can serve as a bridge to quantum crypto algorithms. Since this process will require many years and high costs, hybrid methods can continue to protect the security of existing systems.

6.3. Comparison of Classical and Hybrid Encryption Structures (Klasik ve Hibrit Şifreleme Yapılarının Karşılaştırılması)

The hybrid encryption model proposed in this study was developed based on the prediction that traditional asymmetric structures may be insufficient against quantum threats. The table below presents a comparison of the classical asymmetric encryption structure and the proposed symmetric PSK-supported hybrid model in terms of criteria such as quantum durability, key management, security level and transition process compatibility

Table 2. Comparison of Classical Asymmetric and PSK Supported Hybrid Encryption Structures (Klasik Asimetrik ve PSK Destekli Hibrit Şifreleme Yapılarının Karşılaştırılması)

Feature	Classical	Hybrid (PSK+Asymmetric)
Quantum attack resistance	⚠ Low	✅ High
Key encryption	❌ None	✅ Encrypted with AES
Key distribution protection	❌ Open	✅ Secure channel
Post-quantum preparation	❌ Weak	✅ Strong transition model

This comparison reveals that the proposed structure is particularly capable of serving as a bridge between the pre-quantum and quantum transition periods. An additional security layer is provided against open channel attacks thanks to the symmetrically encrypted asymmetric key parameters.

6.4. Security Assumptions (Güvenlik Varsayımları)

The security of the proposed hybrid encryption structure is built on the following basic assumptions.

Privacy of Symmetric PSK: The symmetric PSK is assumed to be transmitted between the parties in

a secure manner and is known only to the authorized parties. The disclosure of the PSK is a serious risk that will weaken the entire security structure of the proposed system.

AES Based Symmetric Encryption Security: The AES algorithm is assumed to be secure against both classical and quantum attacks. In particular, the use of AES-256 or AES-512 provides sufficient resistance against the Grover algorithm.

Asymmetric Key Integrity: It is assumed that both parties have reliably generated public and private key pairs and obtained the other party's public key with accuracy.

Reliability of Time Codes: It is assumed that PSKs are marked with time codes and that the validity periods of these codes are interpreted correctly by the parties. It is assumed that there is sufficient time synchronization between the parties.

7. CONCLUSION AND RECOMMENDATIONS (Sonuç ve Öneriler)

7.1. Conclusion (Sonuç)

This paper evaluates the potential impact of quantum computers on classical cryptographic methods and proposes a hybrid encryption model that provides additional security measures against these threats. As is well known, widely used asymmetric encryption algorithms such as RSA and ECC can be efficiently solved by quantum computers thanks to the Shor algorithm [1]. This shows that asymmetric systems have serious security vulnerabilities in the quantum era.

On the other hand, symmetric algorithms such as AES exhibit a relatively more resistant structure against quantum computers. Although the Grover algorithm reduces the security of symmetric encryption systems, this situation can be balanced by using longer keys. In this context, the key lengths of AES-256 and above provide a reasonable level of security against quantum attacks.

In the proposed hybrid model, asymmetric keys are protected by additionally encrypting them with a pre-shared symmetric key. This approach creates an additional layer of defense against quantum attacks on asymmetric systems, making the security of classical infrastructures sustainable even in the quantum era. One of the strongest aspects of the model is that it is compatible with the current system architecture and provides temporary but effective protection until the transition to post-quantum algorithms is fully achieved.

The transition process to post-quantum algorithms is expected to be long and costly. In this process, the use of hybrid approaches is of strategic importance for the protection of data integrity and confidentiality, especially for critical infrastructures. In this context, the hybrid encryption model presented in the study offers a solution proposal that increases the resilience of existing systems against the threats posed by quantum computers, is applicable and supports the transition process.

7.2. Recommendations (Öneriler)

In line with the findings obtained as a result of this study, the following recommendations are presented in order to plan an effective transition process against the threats posed by quantum computers.

Standardization of Hybrid Encryption Systems: The proposed PSK-based hybrid encryption model provides an important intermediate solution to ensure the security of existing systems until the transition to post-quantum algorithms is completed. This model should be included in international security standards and supported by sector-based adaptable protocols.

Develop Quantum Security Policies for Critical Infrastructures: The public and private sectors, with a priority on critical infrastructures, should develop comprehensive security policies that include hybrid encryption models. These policies will serve as a roadmap to prepare for post-quantum cryptography.

Increasing Symmetric Encryption Key Lengths: Considering the effects of the Grover algorithm, it is necessary to use AES-256 or higher-level keys instead of AES-128. This strengthening in symmetric algorithms also directly affects the overall security of the hybrid model.

Integration of Post-Quantum Encryption Algorithms: The high cost and time-consuming nature of the transition to post-quantum algorithms necessitates that this transition be carried out gradually and starting from critical systems. In this process, the proposed hybrid model will provide effective transition support.

Increasing Education and Awareness-Raising Activities: Raising awareness of public and private sector personnel on quantum security issues should be supported with training programs and seminars. In this way, institutional and social preparation for the post-quantum era will be strengthened.

DECLARATION OF ETHICAL STANDARDS (ETİK STANDARTLARIN BEYANI)

The author of this article declares that the materials and methods they use in their work do not require ethical committee approval and/or legal-specific permission.

Bu makalenin yazarı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

AUTHORS' CONTRIBUTIONS (YAZARLARIN KATKILARI)

***Fatih SELVİ*:** Creating the Idea of the Study, Literature Research, Creating Methodology, Writing the Original Draft.

Çalışmanın Fikrini Oluşturma, Literatür Araştırma, Metodoloji Oluşturma, Orijinal Taslak Yazımı.

Mustafa ALKAN: Editorial Review, Administration, Supervision.

Yazım İnceleme, Yönetim, Denetim.

CONFLICT OF INTEREST (ÇIKAR ÇATIŞMASI)

There is no conflict of interest in this study.

Bu çalışmada herhangi bir çıkar çatışması yoktur.

REFERENCES (KAYNAKLAR)

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annu. Symp. Found. Comput. Sci., Santa Fe, NM, USA, 1994, pp. 124–134.

[2] National Institute of Standards and Technology (NIST), "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," Aug. 13, 2024. [Online]. Available: https://www.nist.gov/newsevents/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[3] D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper, "Transition to Post-Quantum Cryptography Standards," NIST Interagency/Internal Report (NIST IR) 8547, Nov. 12, 2024. [Online]. Available: https://csrc.nist.gov/pubs/ir/8547/ipd

[4] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: quantum resource estimates," in Lecture Notes in Computer Science, vol. 9562, pp. 29–43, 2016

[5] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," in Advances in Cryptology – ASIACRYPT 2020, Cham: Springer, 2020, pp. 451–481. [Online]. Available: https://eprint.iacr.org/2019/1011.

[6] R. Perlner and D. Moody, "Harvesting and the threat of record now, decrypt later," NIST Cybersecurity White Paper, 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2021/record-now-decrypt-later

[7] Y. Chen, N. Alharthi, M. Kamp, and D. Bernstein, "Hybrid Post-Quantum and Classical Cryptographic Schemes," Cryptology ePrint Archive, 2022. [Online]. Available: https://eprint.iacr.org/2022/205

[8] J. Daemen and V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002

[9] M. E. Hellman, "An overview of public key cryptography," IEEE Communications Magazine, vol. 16, no. 6, pp. 42–49, 1978.

[10] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126. DOI: 10.1145/359340.359342

[11] D. R. Stinson and M. B. Paterson, Cryptography: Theory and Practice, 4th ed., CRC Press, 2019.

[12] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2010

[13] M. S. Kues, J. C. Loredo, and A. G. White, "Quantum Fourier Transform Has Small Entanglement," PRX Quantum, vol. 4, no. 4, p. 040318, 2023. doi: 10.1103/PRXQuantum.4.040318

[14] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," arXiv preprint arXiv:1905.09749, 2019. [Online]. Available: https://arxiv.org/abs/1905.09749. [Accessed: 1-Apr-2025].

[15] A. Dash, D. Sarmah, B. K. Behera ve P. K. Panigrahi, "Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer," arXiv preprint arXiv:1805.10478, 2018. [Online]. Available: https://arxiv.org/abs/1805.10478. [Erişim: 1-Nis-2025]

[16] X. Xu, L. Li, Y. Li, Y. Ma, X. Li, J. Zhang, H. Wang, Y. Liu, Y. Xu, Z. Zhang ve diğerleri, "Experimental quantum factoring of 48-bit semiprimes," Nature, vol. 586, no. 7828, pp. 48-52, 2020. [Online]. Available: https://www.nature.com/articles/s41586-019-1503-0. [Erişim: 1-Nis-2025].

[17] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th ACM Symp. Theory of Computing (STOC)*, 1996, pp. 212–219.

[18] L. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," arXiv preprint arXiv:1910.01700, 2019. [Online]. Available: https://arxiv.org/abs/1910.01700. [Accessed: 1-Apr-2025].

[19] S. D. and P. C., "On the Practical Cost of Grover for AES Key Recovery," Fifth PQC Standardization Conf., NIST, 2024. [Online]. Available: https://csrc.nist.gov/csrc/media/events/2024/fifth-pqc/documents/papers/on-practical-cost-of-grover.pdf

[20] NIST, "Post-Quantum Cryptography: NIST's Plan for the Future," 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/post-quantum-cryptography -nists-plan-future

[21] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Migration to Post-Quantum Cryptography," BSI White Paper, 2023. [Online]. Available: https://www.bsi.bund.de

[22] European Union Agency for Cybersecurity (ENISA), "Post-Quantum Cryptography: Current State and Quantum Threats," 2023. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-report