Classical and post-quantum encryption for GDPR

Maksim Iavich[1,†], Oksana Kovalchuk[2,†], Sergiy Gnatyuk[3,†], Yuliia Khavikova[4,†] and Volodymyr Sokolov[5,*,†]

[1] Caucasus University, 1 Paata Saakadze str., 0102 Tbilisi, Georgia
[2] Sokhumi State University, 61 Politkovskaya str., 0186 Tbilisi, Georgia
[3] National Aviation University, 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine
[4] State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine
[5] Borys Grinchenko Kyiv Metropolitan University, 18/2, Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

In the dynamic digital landscape, the General Data Protection Regulation (GDPR) stands as a transformative force, which aims to secure individual privacy and redefine organizational practices in personal data handling. This paper analyzes the multifaceted layers of GDPR in detail, it elucidates its principles, rights for data subjects, and obligations for data controllers and processors. The main attention is paid to encryption standards, with specific recommendations for data protection in both classical and post-quantum epochs. In the classical setting, the paper aims to employ AES-128 in data storage, striking a balance between security and performance. For communication, the SSL protocol is used, with a caveat to transition to TLS for contemporary applications. In the post-quantum epoch, where there will be fully-fledged quantum computers, the paper proposes a shift to AES-256 for data storage and introduces CRYSTALS-Kyber, an asymmetric cryptography algorithm secure against quantum attacks, for secure communication. The recommendations emphasize the need for creating precise cryptographical recommendations, particularly in the face of evolving threats. Compliance with GDPR and other data protection regulations remains very important, ensuring the security and integrity of data in the 21st century.

Keywords

GDPR, AES-256, encryption, post-quantum cryptography, cryptographical application

1. Introduction

Because of the rapid evolution of digital technologies, the security of data has become very important [1, 2]. As people have to share their personal information online, concerns about data privacy and security have become impor-tant. In response to these concerns, the Euro-pean Union (EU) has elaborated the General Data Protection Regulation (GDPR), a land-mark legislation designed to secure the rights and privacy of individuals in the digital realm.

The GDPR, which came into effect on May 25, 2018, represents a paradigm shift in data protection, emphasizing transparency, accountability, and individual empowerment. Its main goal is to provide individuals with greater control over their data while imposing strict rules on organizations that process such information. Because of the importance of GDPR, this paper aims to analyze the regulatory framework, exploring its fundamental principles, the rights it affords to data subjects and the obligations it places upon data controllers and processors [3–5].

As we study GDPR, it becomes evident that this regulation is not a legal framework but a catalyst for an important organizational shift towards a more privacy-oriented approach. By understanding the nuances and implications of the GDPR, businesses, policymakers, and individuals can actively contribute to the responsible and ethical use of personal data in the digital era [6–8].

This paper studies the multifaceted layers of the GDPR, providing a comprehensive of these layers. Through this exploration, we aim to foster a deeper understanding of the GDPR's significance, its impact on various stakeholders, and the evolving landscape of data protection in the 21st century. The main aim of the paper is to analyze the encryption standards for data protection. Based on the analysis the goal of the paper is to offer a detailed recommendation for data encryption in ongoing and post-quantum epochs.

2. GDPR layers

Let's mention analyze the various layers of the GDPR and their implications:

CQPC-2024: Classic, Quantum, and Post-Quantum Cryptography, August 6, 2024, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
miavich@cu.edu.ge (M. Iavich); oksana.kovalchuk@gmail.com (O. Kovalchuk); s.gnatyuk@nau.edu.ua (S. Gnatyuk); pirogova0303@gmail.com (Y. Khavikova); v.sokolov@kubg.edu.ua (V. Sokolov)

0000-0002-3109-7971 (M. Iavich); 0000-0002-2354-6545 (O. Kovalchuk); 0000-0003-4992-0564 (S. Gnatyuk); 0000-0003-1017-3602 (Y. Khavikova); 0000-0002-9349-7946 (V. Sokolov)

2.1. Principles

Lawfulness, Fairness, and Transparency: This principle ensures that organizations process personal data legally and transparently. It emphasizes the importance of informing individuals about the processing activities and the reasons behind them, fostering trust and accountability.

Purpose Limitation and Data Minimization: These principles emphasize the need for organizations to clearly define the purposes for which they collect data and to collect only the minimum necessary data for those purposes. This helps prevent the indiscriminate collection and processing of personal information.

Accuracy and Storage Limitation: These principles highlight the importance of maintaining accurate and up-to-date data and ensuring that personal data is not stored longer than necessary. This promotes data quality and relevance.

Integrity and Confidentiality: Organizations must implement security measures to protect personal data from unauthorized access, disclosure, alteration, and destruction, ensuring the integrity and confidentiality of the data.

2.2. Data subject rights

The recognition of robust data subject rights empowers individuals to have control over their data. This includes the right to access their information, rectify inaccuracies, and even request the deletion of their data under certain circumstances. These rights enhance individual autonomy and privacy.

2.3. 3. Lawful basis for processing

Requiring a lawful basis for processing ensures that organizations have a legitimate reason for collecting and processing personal data. This prevents arbitrary or unjustified processing and encourages responsible data management.

2.4. Consent

The GDPR introduces a higher standard for obtaining and managing consent. It ensures that individuals are fully informed and have given clear affirmative action, fostering a more transparent and ethically grounded approach to data processing.

2.5. Data protection officer

The appointment of a Data Protection Officer (DPO) is a proactive step toward ensuring that organizations have a designated person responsible for overseeing data protection compliance. This demonstrates a commitment to accountability and effective governance.

2.6. Data processing records

Maintaining records of data processing activities promotes transparency and accountability. It helps organizations keep track of their data processing practices and facilitates cooperation with data protection authorities during audits.

2.7. Data protection impact assessments

Data Protection Impact Assessments (DPIAs) are a proactive tool for identifying and mitigating potential risks associated with data processing activities. This encourages organizations to assess and address privacy risks before initiating certain processing operations, aligning with a risk-based approach to data protection.

2.8. Cross-border data transfers

The restrictions on cross-border data transfers ensure that personal data leaving the EU enjoys an adequate level of protection. This protects the privacy rights of individuals, even when their data is transferred internationally.

2.9. Data breach notification

The mandatory reporting of data breaches within 72 hours enhances transparency and enables swift action to mitigate potential harm. This requirement emphasizes the importance of timely and effective responses to security incidents.

2.10. Accountability and governance

The principles of accountability and governance require organizations to take responsibility for their data processing activities. This involves adopting internal policies, conducting training, and maintaining documentation, fostering a culture of compliance and transparency.

As we can see, the layers of GDPR collectively create an interesting and important framework that prioritizes the rights and privacy of individuals, fosters transparency, and promotes responsible data governance across organizations. Compliance with these layers not only ensures legal adherence but also contributes to a more ethical and trustworthy data ecosystem.

3. Encryption in GDPR

The GDPR does not explicitly mandate the use of specific security technologies like data encryption. However, GDPR does require organizations to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Encryption is recognized as one of the security

measures that can help protect personal data, and it is explicitly mentioned in several articles of the regulation. Here are the four most relevant aspects of GDPR related to data encryption:

1. Security of Processing (Article 32):

Article 32 of the GDPR outlines the security of processing requirements. It states that controllers and processors must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This includes the pseudonymization and encryption of personal data.

2. Pseudonymization (Recital 78):

Recital 78 of the GDPR specifically mentions pseudonymization as a security measure. Pseudonymization is a process that involves replacing or encrypting personal data in a way that prevents attributing it to a specific data subject without additional information.

3. Notification of a Personal Data Breach to the Supervisory Authority (Article 33):

In the event of a personal data breach, Article 33 requires the data controller to notify the supervisory authority without undue delay, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Encryption is mentioned as a measure to mitigate the risks associated with a data breach.

4. Communication of a Personal Data Breach to the Data Subject (Article 34):

Article 34 states that, in certain cases, the data controller is required to communicate the personal data breach to the data subject without undue delay. However, this communication is not necessary if the data is unintelligible due to encryption or other security measures.

In summary, while GDPR doesn't explicitly mandate data encryption, it strongly encourages its use as part of a broader set of security measures. The implementation of encryption, especially when combined with other security practices like pseudo-nymization, helps organizations meet the GDPR's requirements for securing personal data and mitigating the risks associated with data breaches. Organizations should assess the risks associated with their data processing activities and implement security measures, including encryption, based on the principle of proportionality.

4. Problem statement and solution

As we can see GDPR does not explicitly mandate data encryption. Without the recommendation of concrete encryption standards, it is complicated for organizations to choose the needed standards. It can lead to security breaches. For the local data storage, we can use symmetric encryption.

AES, which stands for Advanced Encryption Standard, is a widely used symmetric encryption algorithm that plays a crucial role in securing data, including its storage. AES was established as a standard by the National Institute of Standards and Technology (NIST) in 2001, replacing the Data Encryption Standard (DES). AES is known for its efficiency, security, and versatility, making it a popular choice for encrypting sensitive information.

Here are key aspects of using AES as a method for storing data [9]:

AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. This simplicity in key management makes AES efficient for storing and retrieving encrypted data. AES supports key lengths of 128, 192, and 256 bits. Longer key lengths generally provide stronger security, but they may require more computational resources. The choice of key length depends on the desired level of security and the specific implementation.

AES operates as a block cipher, encrypting data in fixed-size blocks. The standard block size for AES is 128 bits. Each block undergoes multiple rounds of encryption and transformation, contributing to the algorithm's security.

AES can be used in various modes of operation, such as Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and others. The mode of operation determines how the algorithm encrypts data blocks and adds a layer of complexity and security.

The cryptosystem is commonly employed for data-at-rest encryption, securing data stored on devices such as hard drives, SSDs, and other storage media. Encrypting data at rest helps protect sensitive information from unauthorized access, especially in the event of physical theft or data breaches.

AES is often used to meet various security and compliance standards, including those related to data protection and privacy. Its acceptance as a secure encryption algorithm by international organizations and regulatory bodies makes it a suitable choice for organizations handling sensitive data.

AES encryption can be also integrated into various storage systems, including databases and file systems. This integration allows organizations to encrypt data at the storage level, providing an additional layer of protection beyond application-level encryption.

The cryptosystem is designed to be computationally efficient, but the performance impact of encryption can vary based on factors such as key length, mode of operation, and the hardware used. Modern processors often include hardware acceleration for AES, optimizing performance.

IT must be mentioned, that effective key management is crucial when using AES. Safeguarding encryption keys is essential to maintaining the security

of encrypted data. Organizations should implement secure key storage and distribution practices.

Choosing Advanced Encryption Standard (AES) for GDPR Compliance in the realm of General Data Protection Regulation (GDPR) compliance, the selection of a robust encryption standard is obligatory for securing personal data. As we mentioned above it stands out as a highly secure and good choice that aligns with GDPR principles. AES, a symmetric encryption algorithm, has earned its reputation for security through rigorous cryptographic analysis. Its implementation provides sufficient protection for sensitive information, addressing the GDPR's mandate for robust data protection. Especially well-suited for encrypting stored information, AES's symmetric nature ensures efficient and effective encryption, meeting GDPR's emphasis on securing data at rest. This approach guarantees that personal data remains confidential and protected from unauthorized access. The cryptosystem aligns seamlessly with GDPR principles, including data minimization, integrity, and confidentiality. By employing AES for data encryption, organizations adhere to GDPR's mandate to store and manage only necessary information while maintaining data integrity and confidentiality through encryption. In the unfortunate event of a data breach, GDPR necessitates prompt notification to the supervisory authority and, in certain cases, to data subjects. The cryptosystem plays an important role in breach mitigation by rendering the encrypted data unreadable without the proper decryption key, reducing the risk of harm to individuals. GDPR encourages the use of pseudonymization as an additional security measure. AES, integrated into a broader pseudonymization strategy, adds an extra layer of complexity, making it challenging to associate encrypted data with specific individuals without the requisite decryption keys. Widely adopted across industries, AES's versatility allows for seamless integration into various systems, databases, and storage solutions. Its international recognition contributes to a consistent and effective approach to data encryption, aligning with GDPR's emphasis on protecting personal data regardless of geographical boundaries.

Therefore, selecting AES as the encryption standard for GDPR compliance reflects a commitment to the secure processing and storage of personal data. While encryption is a crucial aspect of GDPR compliance, organizations should adopt a holistic approach, considering additional technical and organizational measures to ensure comprehensive data protection. The key size can be chosen as a 128-bit length.

For communication encryption, we offer to use asymmetric encryption. Using SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security), for data transfer is a common and recommended practice to ensure the secure transmission of data, and it aligns well with GDPR requirements for protecting personal data during transit [10]. Here's an overview of how SSL/TLS can be considered as an encryption standard for GDPR compliance:

SSL/TLS protocols are designed to provide a secure channel for data transmission over the internet. This is achieved through encryption, which protects the confidentiality and integrity of the data being transferred between a user's browser and a web server. GDPR emphasizes the principles of data protection, including the need to process personal data securely. Using SSL/TLS for data transfer helps organizations comply with these principles by ensuring that sensitive information is encrypted during transmission, preventing unauthorized access or interception.

SSL/TLS protocols use strong encryption algorithms to secure data. The choice of encryption algorithms and key lengths in the configuration of SSL/TLS can be aligned with GDPR's emphasis on adopting appropriate technical measures to protect personal data.

GDPR grants individuals the right to have their data processed securely. By implementing SSL/TLS, organizations contribute to the protection of data subject rights, especially during data transfer processes where the risk of interception is higher.

SSL/TLS contributes to secure communication between data subjects and data controllers. When obtaining consent or communicating with individuals regarding their data, the use of encrypted channels helps maintain the confidentiality and integrity of the information exchanged.

The protocol not only encrypts data but also provides a mechanism for server authentication. Verifying the identity of the server helps prevent man-in-the-middle attacks, ensuring that data is transmitted to and from legitimate sources.

In the event of a personal data breach, GDPR mandates timely notification. The use of SSL/TLS can mitigate the risk of data breaches during transmission, reducing the likelihood of unauthorized access and the need for such notifications.

The protocol is considered a standard and best practice for securing data in transit. Its widespread adoption across the internet and acceptance as a secure communication protocol contribute to its alignment with industry standards, reinforcing its suitability for GDPR compliance.

It's important to note that while SSL/TLS is crucial for securing data in transit, a comprehensive GDPR compliance strategy should encompass other security measures, including encryption at rest, access controls, and secure data processing practices. Additionally, organizations should stay informed about evolving

encryption standards and vulnerabilities to ensure the ongoing effectiveness of their security measures.

5. Secure encryption under GDPR

5.1. Encryption as a security measure

Article 32 of the GDPR explicitly mentions encryption as a security measure that organizations should consider to protect personal data. Encryption helps ensure the confidentiality, integrity, and availability of data by making it unreadable to unauthorized parties.

While encryption is not mandatory, it is strongly recommended, especially for protecting sensitive data. The GDPR promotes a risk-based approach, where encryption is one of the methods to mitigate risks to personal data.

5.2. Data breach notification

Under Article 34, if a data breach occurs and the personal data is encrypted, the breach is less likely to pose a high risk to the rights and freedoms of individuals. As a result, if the data is properly encrypted, organizations might not need to notify the affected individuals, provided the encryption is robust and the decryption key has not been compromised.

5.3. Data protection by design and by default

Article 25 encourages organizations to implement appropriate technical and organizational measures, such as encryption, from the outset of data processing activities. This concept, known as "data protection by design and by default", aims to integrate privacy features directly into the processing systems and services.

5.4. Pseudonymization

Encryption is often used as a tool for pseudonymization, a process mentioned in GDPR that reduces the risks to data subjects. Pseudonymization involves processing personal data in such a manner that it cannot be attributed to a specific individual without additional information, which must be kept separately and securely.

5.5. Impact on data processing

When data is encrypted, it may affect how it can be processed. For instance, encrypted data typically cannot be searched or analyzed in its encrypted form, which may necessitate the development of secure and efficient decryption processes within an organization.

6. Solution for post-quantum epoch

Grover's algorithm is a quantum algorithm that addresses the problem of unstructured search, and it has implications for symmetric-key cryptography, including algorithms like AES. Grover's algorithm offers a quadratic speedup for unstructured search problems [11].

In the context of symmetric-key cryptography, Grover's algorithm can be used to search an unsorted database or find the key for a symmetric encryption algorithm. Grover's algorithm implies that the time complexity of a brute-force search is reduced from $O(2^n)$ to $O(2^{n/2})$, where "n" is the key length. This means that the security strength provided by a key length of "n" bits against a brute-force search is halved when subjected to Grover's algorithm.

For example, if you have a symmetric key with a length of 128 bits, classically it would take an exhaustive search of 2^{128} operations to find the key. With Grover's algorithm, the time complexity is reduced to the square root of 2^{128}, which is 2^{64} operations. Therefore, the effective security strength is reduced to 64 bits against a quantum search. To maintain a certain level of security against quantum attacks, it's generally recommended to use longer key lengths with symmetric key algorithms. For instance, if you were aiming for 128-bit security against a quantum attack, you might use a key length of 256 bits with a symmetric algorithm like AES.

Therefore, we offer to use the key length of 256 bits for AES to securely store data.

For communication asymmetric cryptography must be involved. Quantum computers can break the existing asymmetric cryptography using Shor's algorithm [12].

Shor's algorithm is a quantum algorithm designed to efficiently factorize large numbers and compute discrete logarithms, which poses a significant risk to widely used encryption methods like RSA and ECC. In particular, RSA's security, dependent on the difficulty of factoring large numbers, and ECC, relying on the elliptic curve discrete logarithm problem, are compromised by Shor's algorithm on a sufficiently powerful quantum computer [13, 14].

On a different front, Grover's algorithm, a quantum search algorithm, has implications for symmetric encryption and impacts the effective key length. While not directly breaking public-key cryptography, Grover's algorithm provides a quadratic speedup for unstructured search problems, effectively halving the security provided by symmetric encryption key lengths. This prompts the need for longer key lengths in symmetric encryption to maintain equivalent security levels in the face of quantum threats [15–17].

To counter these quantum risks, ongoing efforts in post-quantum cryptography are focused on developing encryption algorithms resistant to quantum attacks. Researchers are exploring alternative mathematical problems and cryptographic techniques to ensure the continued security of digital communication in a quantum computing era.

Therefore, for asymmetric encryption, we offer to use already existing NIST standards. GAITHERSBURG, Md.—The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, has taken a significant step in addressing the potential threat posed by future quantum computers to digital security. NIST has unveiled the initial group of encryption tools designed to withstand quantum computer attacks, which could jeopardize the privacy of information crucial to daily digital activities such as online banking and email communication. These selected encryption algorithms are anticipated to be part of NIST's forthcoming post-quantum cryptographic standard, expected to be finalized within approximately two years.

Gina M. Raimondo, the Secretary of Commerce, emphasized the importance of this announcement as a milestone in fortifying sensitive data against potential cyber threats from quantum computers. NIST has played a crucial role in managing a six-year effort that began in 2016, urging cryptographers globally to create and vet encryption methods capable of resisting attacks from more powerful quantum computers. The unveiling of these encryption algorithms marks a pivotal stage in NIST's post-quantum cryptography [18] standardization project.

Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio highlighted NIST's forward-looking approach to anticipate the needs of U.S. industry and society. The agency's post-quantum cryptography program, drawing on top cryptography experts worldwide, has produced the first set of quantum-resistant algorithms aimed at establishing a standard to significantly enhance digital information security. This initial selection includes four encryption algorithms designed to resist quantum attacks. Four additional algorithms are currently under consideration, with the finalists expected to be announced in the future. The decision to reveal choices in two stages is driven by the necessity for a diverse range of defense tools. Different systems and tasks utilizing encryption demand tailored solutions, diverse approaches, and multiple algorithms to address potential vulnerabilities.

It must be mentioned that encryption is a fundamental mechanism that employs mathematical principles to safeguard electronic information and faces a potential challenge from quantum computers. Unlike conventional computers, quantum computers could rapidly solve math problems currently deemed intractable, rendering existing encryption systems vulnerable. The selected quantum-resistant algorithms, designed for general encryption and digital signatures, rely on math problems that both conventional and quantum computers should find challenging to solve. The chosen algorithm for general encryption is CRYSTALS-Kyber, recognized for its smaller encryption keys facilitating easy exchange between parties and operational speed [19–24].

Therefore, we offer to use CRYSTALS-Kyber as asymmetric encryption.

7. Final recommendations for NIST encryption standards

Classical setting:

1. Data Storage (AES-128):

Using AES-128 for data storage is a common and secure practice. It provides a good balance between security and performance in most scenarios.

2. Communication (SSL Protocol):

SSL (Secure Sockets Layer) has been widely used for securing communication over the internet. Note that the latest version of SSL is TLS (Transport Layer Security), and it's recommended to use TLS instead for modern applications [24–26].

Post-Quantum Epoch:

Data Storage (AES-256):

In a post-quantum epoch, where quantum computers may pose a threat to certain cryptographic algorithms, it's prudent to use a higher key size for encryption. AES-256 provides stronger security compared to AES-128 and is considered more resilient to potential quantum attacks.

Communication (Asymmetric Cryptography—CRYSTALS-Kyber):

In a post-quantum era, asymmetric algorithms may become vulnerable to attacks by quantum computers. As a result, using asymmetric cryptography that is considered quantum-resistant becomes essential. CRYSTALS-Kyber is a post-quantum key exchange algorithm, and choosing it for communication aligns with the goal of future-proofing against quantum threats.

It's important to stay informed about the latest developments in cryptography and regularly update cryptographic protocols and algorithms to maintain the security of data in changing threat landscapes. Additionally, compliance with relevant data protection regulations, such as GDPR, should always be considered in cryptographic decisions [27–30].

The pseudo-code for the usage of the offered technologies can look as follows:

```
# Import necessary cryptographic libraries
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, and modes
from cryptography.hazmat.backends import default_backend
from crystals_kyber import kyber

# Function to generate AES key based on epoch
def generate_aes_key(epoch):
    if epoch == "classical":
        return generate_aes_key_classical()
    elif epoch == "post_quantum":
        return generate_aes_key_post_quantum()
    else:
        raise ValueError("Invalid epoch specified")

# Function to generate AES-256 key for classical setting
def generate_aes_key_classical():
    # Implement the key generation for the classical setting
    pass

# Function to generate AES-256 key for post-quantum epoch
def generate_aes_key_post_quantum():
    # Implement the key generation for the post-quantum epoch
    pass

# Function to encrypt data based on epoch and usage
def encrypt_data(data, epoch, usage):
    if epoch == "classical":
        if usage == "storage":
            return encrypt_data_aes(data, generate_aes_key_classical())
        elif usage == "communication":
            return secure_communication_classical(data)
        else:
            raise ValueError("Invalid usage specified")
    elif epoch == "post_quantum":
        if usage == "storage":
            return encrypt_data_aes(data, generate_aes_key_post_quantum())
        elif usage == "communication":
            return secure_communication_post_quantum(data)
        else:
            raise ValueError("Invalid usage specified")
    else:
        raise ValueError("Invalid epoch specified")

# Function to encrypt data using AES-256
def encrypt_data_aes(data, key):
    cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=default_backend())
    encryptor = cipher.encryptor()
    encrypted_data = encryptor.update(data) + encryptor.finalize()
    return encrypted_data

# Function to perform secure communication in a classical setting
def secure_communication_classical(data):
    # Implement TLS/SSL with RSA or ECC
    pass

# Function to perform secure communication with post-quantum epoch
def secure_communication_post_quantum(data):
    # Implement CRYSTALS-Kyber for key exchange
    pass

# Example usage:
plaintext_data = "Sensitive data to be encrypted."
epoch = "post_quantum" # Change this to "classical" for the classical setting
usage = "communication" # Change this to "storage" for data storage

# Encryption based on the specified epoch and usage
encrypted_data = encrypt_data(plaintext_data, epoch, usage)

# Now, encrypted_data can be stored or transmitted securely.
```

8. Conclusions and future plans

Cryptography is an essential tool for GDPR compliance, providing the means to protect personal data effectively. By implementing strong cryptographic measures, organizations can significantly reduce the risk of data breaches and ensure that they meet the stringent requirements of the GDPR. The best practices for Using Cryptography under GDPR are the following:

- Key Management: Proper management of encryption keys is critical to ensuring that encrypted data remains secure. Keys must be stored and managed securely to prevent unauthorized access.
- Regular Audits and Updates: Cryptographic algorithms and their implementations should be regularly audited and updated to protect against emerging threats.
- Compliance with Standards: Use cryptographic methods that comply with recognized standards, such as those from the NIST or the European Telecommunications Standards Institute (ETSI).

In conclusion, our cryptographic recommendations aim to establish a robust and adaptable security foundation for our system. For data storage in the classical epoch, we offer to use of AES-128, a widely recognized and efficient symmetric encryption algorithm. This choice strikes a balance between security and computational efficiency, making it suitable for protecting stored data in various scenarios.

For secure communication, we recommend the use of SSL/TLS protocols, incorporating modern cipher suites such as those based on AES in combination with RSA or ECC for key exchange. SSL ensures the confidentiality and integrity of data during transmission, and our approach aligns with current best practices for secure communication.

In anticipation of future challenges posed by quantum computing, our transition to post-quantum algorithms is exemplified by the adoption of CRYSTALS-Kyber for secure communication. This step reflects our commitment to staying ahead of emerging threats and safeguarding sensitive information.

In our future research, we think of offering the post-quantum model for SSL.

Acknowledgment

This work was funded by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060).

References

[1] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021) 213–217. doi: 10.1109/picst54195.2021.9772181.

[2] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: 8th International Conference on "Mathematics. Informa-tion Technologies. Education:" Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[3] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecom-munications Network, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 240–245.

[4] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.

[5] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[6] H. Li, Yu L., H. Wu, The Impact of GDPR on Global Technology Development, J. Global Inf. Technol. Manag. 22(1) (2019) 1–6. doi: 10.1080/ 1097198X.2019.156 9186.

[7] C. Tankard, What the GDPR Means for Businesses, Netw. Secur. 2016(6) (2016) 5–8. doi: 10.1016/S1353-4858(16)300 56-3.

[8] G. Johnson, S. Shriver, S. Goldberg, Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR, Manag. Sci. 69(10) (2023) 5695–6415. doi: 10.1287/mnsc.2023. 4709.

[9] J. Daemen, V. Rijmen, AES Proposal: Rijndael (1999).

[10] D. Wagner, B. Schneier, Analysis of the SSL 3.0 Protocol, The Second USENIX Workshop on Electronic Commerce Proceedings 1(1) (1996).

[11] R. Jozsa, Searching in Grover's Algorithm (1999). doi: 10.48550/arXiv.quant-ph/9901021.

[12] T. Monz, et al., Realization of a Scalable Shor Algorithm, Science 351(6277) (2016) 1068–1070. doi: 10.1126/scien ce.aad9480.

[13] H. Wong, Shor's Algorithm, Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps. Cham: Springer International Publishing (2023) 289–298.

[14] A. M. Patoary, et al., Chaotic Roots of the Modular Multiplication Dynamical System in Shor's Algorithm (2023). doi: 10.48550/arXiv.2306.16446.

[15] Z. Hu, et al., High-Speed and Secure PRNG for Cryptographic Applications, Int. J. Comput. Network Inf. Secur. 12(3) (2020) 1–10. doi: 10.5815/ijcnis.2020. 03.01.

[16] M. Iavich, et al., Lattice based Merkle, in: International Conference on Information Technologies, vol. 2470 (2019) 13–16.

[17] S. Tynymbayev, et al., Modular Reduction Based on the Divider by Blocking Negative Remainders, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences 2(434) (2019) 238–248. doi: 10.32014/2019.2518-170x.60.

[18] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[19] M. Iavich, T. Kuchukhidze, R. Bocu, A Post-Quantum Digital Signature Using Verkle Trees and Lattices, Symmetry 15(12) (2023) 2165.

[20] M. Iavich, T. Kuchukhidze, Digital Signature Design Using Verkle Tree (2023).

[21] E. Dubrova, et al., Breaking a Fifth-order Masked Implementation of Crystals-kyber by Copy-paste, Proceedings of the 10th ACM Asia Public-Key Cryptography Workshop (2023).
[22] R. Avanzi, et al., CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation, NIST PQC Round 2(4) (2019) 1–43.
[23] M. Moraitis, et al., Securing CRYSTALS-Kyber in FPGA Using Duplication and Clock Randomization, IEEE Design & Test (2023).
[24] S. Gnatyuk, et al., New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing (2020) 93–104.
[25] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.
[26] S. Gnatyuk, et al., Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, 16th International Conference on Control, Automation and Systems (2016) 1476–1479. doi: 10.1109/iccas.2016.7832498.
[27] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187(1) (2022) 302–309.
[28] C. Papamanthou, et al., Streaming Authenticated Data Structures, Advances in Cryptology—EUROCRYPT (2013) 353–370. doi: 10.1007/978-3-642-38348-9_22.
[29] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.
[30] I. Khaburzaniya, et al., Aggregating and Thresholdizing Hash-Based Signatures Using STARKs, ACM Asia Conf. Comput. Commun. Secur. (2022) 393–407. doi: 10.1145/3488932.3524128.