DOI 10.15276/imms.v14.no1-2.12
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 12-23

HYBRID ASYMMETRIC CODE-BASED CRYPTOSYSTEM

A.Ya. Davletova

West Ukrainian National University,
11, Lvivska Str. Ternopil, 46009, Ukraine
email: a7davletova@gmail.com

This work addresses the pressing issue of ensuring reliable information protection amidst increasing data volumes and rising numbers of cyber threats. Traditional cryptographic systems, while generally reliable, may prove vulnerable to new types of attacks, especially quantum ones. This highlights the need for exploring and researching more resilient encryption methods. The work proposes a hybrid cryptosystem that combines the McEliece system with the RSA encryption algorithm. This approach leverages the advantages of both methods: the high security level of RSA, based on the difficulty of factoring large numbers, and the resilience of McEliece to quantum attacks due to the complexity of decoding arbitrary linear codes. A distinctive feature of the proposed hybrid system is the use of Galois fields *GF(p)* for all operations, which provides an additional layer of protection and flexibility compared to traditional systems based on binary numeral systems. The integration of two asymmetric cryptographic algorithms, whose resilience is based on solving different mathematical problems, enhances the reliability and security of the proposed system. The use of a common parameter *n* for key generation also simplifies key management and expands the key space by a factor of *n*. This solution combines error protection with cryptographic security, making it a powerful tool for data protection in environments with potentially unreliable communication channels. The research conducted as part of this work focuses on analyzing the effectiveness and security of the proposed hybrid cryptosystem. Special attention is given to characteristics such as relative information transmission speed, ciphertext length, key size, and resistance to cryptanalysis. The results demonstrate the advantages of the hybrid system compared to using each algorithm individually. The findings could form the basis for further development of cryptographic methods for information protection in the face of modern threats.
Keywords: McEliece cryptosystem, RSA encryption algorithm, finite fields of Galois, hybrid cryptosystem, resistance to cryptanalysis.

Introduction. The modern world is increasingly reliant on robust information protection methods that ensure data confidentiality, integrity, and authenticity. With the development of digital technologies and the increase in data volumes transmitted through open communication channels, there is a need to improve existing cryptographic systems. One promising direction in cryptography that can provide the necessary level of security with enhanced efficiency is hybrid systems that combine the advantages of different encryption algorithms.

Traditional cryptographic systems can be vulnerable to new types of attacks, necessitating the development of more resilient encryption methods. Furthermore, many existing encryption algorithms are considered vulnerable to quantum computers. Therefore, researching and developing cryptographic methods that are resistant to both classical and quantum cryptanalysis is a pressing task. The solution to this problem is possible through the integration of the McEliece code-based cryptosystem and the asymmetric RSA encryption algorithm, which allows for the creation of more robust, flexible, and efficient cryptographic solutions that meet modern information protection requirements.

In particular, the combination of RSA and the McEliece cryptosystem using Galois fields *GF(p)* and arithmetic operations in these fields is a promising approach that allows the advantages of both methods to be combined, enhancing encryption efficiency and resilience. McEliece, due to its resistance to quantum attacks, and RSA, based on the complexity of factoring large numbers, form the basis for an effective hybrid cryptosystem.

Analysis of research and publications. Compliance with data protection standards requires the implementation of the most advanced encryption methods, driving the research and adoption of new cryptographic techniques. The use of open communication channels for transmitting confidential information, storing data in digital environments, the increase in cyber-attacks, and information misuse create additional requirements for data security. Hybrid cryptosystems, which combine the robustness and efficiency of various encryption algorithms, can offer optimal solutions for enhancing security and efficiency under these conditions.

The security of most widely used cryptosystems is based on the difficulty of solving specific mathematical problems, such as the factorization of large numbers, discrete logarithms, the use of cryptographic hash functions, lattice-based methods, and others [1-4]. Code-based cryptosystems have limited practical application due to implementation complexity and key sizes. However, given the capabilities of quantum computers, particularly their computational speed, these cryptosystems represent a promising and rapidly developing field [5-8].

The potential applications and development of hybrid cryptographic systems are one of the important areas of research [9-11]. Traditional encryption methods, although quite reliable, can become vulnerable to new types of attacks. Hybrid cryptosystems provide greater resilience and information security by leveraging the strengths of traditional methods while compensating for their weaknesses. This underscores the necessity of exploring and researching alternative and hybrid cryptographic systems.

One of the most studied cryptographic systems is the McEliece scheme, based on error-correcting codes [12-17]. It is known for its ability to control and correct errors in the channel and its resistance to attacks. The system is based on an encryption method that uses matrix multiplication to create keys. The main idea is to use linear codes for encryption, where the generating matrix of the code G is multiplied with random matrices S and P, which form the secret key G', to create the public key. This approach ensures data security based on the properties of linear codes and the complexity of recovering the secret key. Decoding requires the use of complex algorithms, the complexity of which grows exponentially with the key size. This problem is considered NP-complete, as there is no efficient algorithm that can find a solution in polynomial time. This makes McEliece resistant to many classical cryptanalysis methods, including potential attacks using quantum computers.

An analysis of the sources allows us to conclude that the search for new data protection methods in the context of post-quantum cryptography, which is based on new mathematical constructions such as code superpositions, is becoming a relevant alternative for future information security.

Typically, hybrid cryptosystems combine the efficiency of symmetric encryption with the security of asymmetric encryption [18-20]. These systems use the best characteristics of both methods to protect data exchange over potentially insecure channels. Combining two encryption approaches, based on different mathematical problems and methods, will provide a higher level of security. Specifically, McEliece uses encoding based on linear codes, while RSA employs asymmetric encryption based on the difficulty of factoring large numbers into primes. The security of RSA may be threatened by the development of quantum computers, whereas McEliece is considered a post-quantum system. The complexity of decrypting both cryptographic systems grows exponentially relative to the key length, which is considered an NP-hard problem.

The combination of the McEliece cryptosystem and the RSA encryption algorithm demonstrates significant potential for ensuring a high level of security in modern cyber threat conditions, as each of these algorithms has its unique advantages: McEliece's resistance to quantum computing and RSA's resistance to classical attacks. The use of characteristics and operations in the Galois field $GF(p)$ further enhances the efficiency and security of the hybrid system. This approach will provide an additional level of cryptographic protection for use in

information security systems and represents a promising direction for research.

The aim of this work is to enhance the reliability of data encryption systems by integrating algorithms whose robustness is based on solving different mathematical problems.

Hybrid Asymmetric Cryptosystem. The proposed hybrid asymmetric cryptosystem is based on the principles of data encoding according to the McEliece scheme using the algebraic structures of Galois fields *GF(p)* and the RSA encryption algorithm. The modified McEliece cryptosystem in *GF(p)* includes the following steps [12]:

1. Key Generation. Selection of the Generating Matrix G. The dimension of G corresponds to the length of the codeword $r \times n$, where $n = k + r$, k is the number of information symbols, and r is the number of check symbols. An $n \times n$ permutation matrix P is used to reorder the symbols in the codeword. A $k \times k$ secret matrix S is chosen from the elements of *GF(p)* and is used for additional mixing of the message symbols before encoding them. The public key G' is computed as follows:

$$G' = SGP.$$

2. Encoding the original message m by transforming it into the codeword x using the public key matrix G':

$$x = mG'.$$

3. Message Transmission. To provide additional protection, an error vector e can be added to the resulting codeword x. In this case, it can be considered an additional one-time secret key. The weight of the error may exceed the boundaries of *GF(p)* since arithmetic operations performed during decryption include normalizing values to the limits of *GF(p)*. However, it will determine the complexity of decoding the corrupted codeword x'. The error correction process uses the principles of the McEliece system, based on the Hamming error-correcting code.

4. Decryption. Upon receiving the codeword x', which contains an error, the private keys P' and S', which are the inverses of the matrices P and S respectively, are used for decoding, where S' is computed in the Galois field *GF(p)*.

$$S' = S^{-1} \, mod \, (p).$$

Restoration of the original message

$$m = x' \, P' \, S'.$$

Using the Galois Field *GF(p)* in the McEliece scheme offers several advantages compared to traditional implementations in binary numeral systems. Operations in *GF(p)* require fewer computational resources compared to operations on binary strings in a binary system, which is crucial in cryptographic applications where computational efficiency can be critical, especially for large message lengths. Using *GF(p)* allows for a larger key size without compromising resistance to attacks, thereby increasing the amount of information that can be transmitted using the McEliece cryptosystem while maintaining the same level of security.

The RSA encryption algorithm includes the following steps [1]:

1. Key Generation. Select two large random prime numbers, p and q. Compute the modulus n as the product of p and q:

$$n = p \cdot q.$$

Computing the Euler's Totient Function $\varphi(n) = (p-1)(q-1)$.

Choosing the public exponent e, which is an integer satisfying the condition $1 < e < \varphi(n)$ and is coprime with $\varphi(n)$.

Calculating the private exponent d as the multiplicative inverse of e modulo $\varphi(n)$:

$$d \cdot e \equiv 1\big(mod \, \varphi(n)\big).$$

2. Encrypting the message m involves computing the ciphertext. c:

$$c = m^e \, mod(n).$$

3. Decrypting c involves computing m:

$$m = c^d \, mod(n).$$

The RSA algorithm allows for secure encryption and decryption of messages using the public *(e, n)* and private *(d, n)* keys.

The integration of the modified McEliece cryptosystem, based on linear codes in the Galois Field *GF(p)*, and the RSA encryption algorithm is realized by using one of the RSA modules *p*, *q*, or their product *n* as the size of the field. Using *n* as the maximum value for the Galois Field parameter in McEliece means that the matrix *S* can include elements that are components of *GF(n)*, thereby increasing the complexity of encoding. This significantly expands the dictionary from 0 to *n*-1, representing the set of possible keys or matrices used for message encoding and decoding. It also allows for the use of more values to represent data in constructing more complex and resistant cryptographic systems.

The algorithm of the proposed hybrid asymmetric cryptosystem based on codes is provided in the figure. 1.

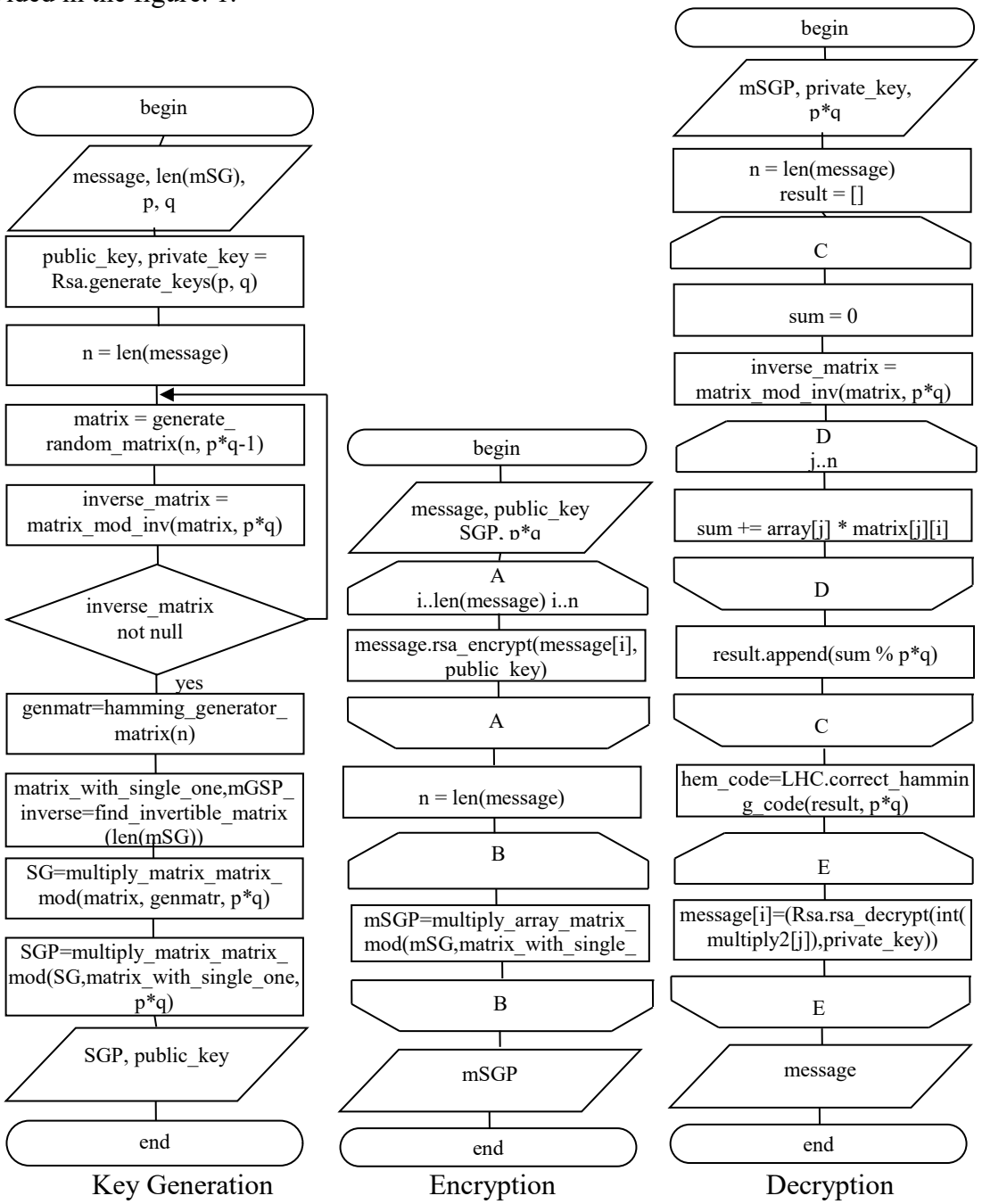

Fig. 1. The algorithm of operation of the hybrid cryptosystem.

For demonstration of the algorithm provided, let's consider an example. Let the plaintext message:

$$m = 9, 5, 11, 28.$$

1. Encryption using RSA:

p=7; q=13; n=91; $\phi(n)$=72; e=5; d=29.

The encrypted message:

$$m' = 81, 31, 72, 84.$$

2. McEliece Encoding. Private Key Generation:

$$G = \begin{matrix} 1110000 \\ 1001100 \\ 0101010 \\ 1101001 \end{matrix} \qquad S = \begin{matrix} 15\ 3\ 35\ 71 \\ 82\ 56\ 18\ 12 \\ 82\ 36\ 40\ 82 \\ 24\ 11\ 9\ 9 \end{matrix} \qquad P = \begin{matrix} 0010000 \\ 1000000 \\ 0000010 \\ 0100000 \\ 0001000 \\ 0000001 \\ 0000100 \end{matrix}$$

Public Key:

$$G' = \begin{matrix} 30\ 18\ 89\ 3\ 71\ 15\ 35 \\ 21\ 86\ 59\ 56\ 12\ 82\ 18 \\ 22\ 67\ 18\ 36\ 82\ 82\ 40 \\ 42\ 29\ 44\ 11\ 9\ 24\ 9 \end{matrix}$$

As a result of encoding, we obtain the message

$$x = 3, 9, 16, 35, 43, 29, 22.$$

Adding an error vector

$$e = 0\ 0\ 21\ 0\ 0\ 0\ 0.$$

We obtain a message corrupted by errors

$$x' = 3, 9, 37, 35, 43, 29, 22.$$

3. Decoding. Computing the inverse matrices S and P:

$$S' = \begin{matrix} 58\ 82\ 53\ 22 \\ 1\ \ 6\ 26\ \ 0 \\ 76\ 49\ 87\ 49 \\ 31\ 89\ 23\ 34 \end{matrix} \qquad P' = \begin{matrix} 0100000 \\ 0001000 \\ 1000000 \\ 0000100 \\ 0000001 \\ 0010000 \\ 0000010 \end{matrix}$$

Restoring the order of symbols in the message x′ P' = 37, 3, 29, 9, 35, 22, 43

Determining error position by recalculating and comparing parity symbols:

p1	16	37
p2	3	3
p3	9	9

As a result, we obtain the binary error position value 100, which corresponds to position 1. In this case, no correction is needed since this position contains a parity symbol.

Information symbols: $m'S'$ = 81, 31, 72, 84.

4. RSA Decryption: m = 9, 5, 11, 28.

The proposed hybrid asymmetric cryptosystem provides additional protection and complexity against cryptanalysis. Combining systems based on different mathematical principles, notably McEliece utilizing coding theory in the Galois field *GF(p)*, where operations are performed on field elements, while RSA employs modular arithmetic operations with large prime numbers, complicates cryptanalytic attacks and ensures a high level of security.

McEliece and RSA serve different application scenarios. McEliece is known for its resistance to lattice-based attacks and quantum computers, whereas RSA is efficient for encrypting short messages and digital signatures. Combining these two methods preserves McEliece's resilience while leveraging RSA's efficiency for rapid encryption of short messages.

The ability to choose the field size provides flexibility in configuring cryptographic

parameters, as the values of p and q depend on specific security and system efficiency requirements. This enables achieving optimal efficiency in cryptographic applications.

Research of the Proposed Cryptosystem. Comparing the efficiency of cryptosystems, we will use criteria such as relative transmission speed, ciphertext length, key size, and resistance to cryptanalysis for each variant.

Relative transmission speed - the ratio of useful information volume to the total volume of transmitted data per unit of time, including all overheads associated with cryptography [21].

For the McEliece scheme, which uses Hamming codes to ensure cryptographic security, the plaintext size is k bits, and the ciphertext size is x, where $x > k$. Efficiency is determined as follows:

$$E_{\text{McEliece}} = \frac{k}{x}.$$

This indicator characterizes the degree of utilization of error-correcting code information capabilities in sequences of length n. For the McEliece cryptosystem in the Galois field $GF(p)$, $E_{McEliece\_}$ is defined similarly as the ratio of information quantity k to the length of the codeword x.

For the RSA algorithm, the relative data transmission speed is determined by the ratio between the key size n and the size of the original message k bits. A larger key size allows for encrypting or decrypting more information simultaneously

$$E_{RSA} = \frac{k}{n}.$$

The size of the plaintext k is limited by the modulus size n, i.e., $k < n$, and the encrypted message x will be almost equal to the size of the modulus n. Therefore, the data transmission efficiency approaches 1.

Table 1 presents the results of conducted research reflecting the relative data transmission speed E at different values of plaintext k and encrypted message x.

Table 1

Relative Data Transmission Speed

k	x	$E_{McEliece}$	E_{Hybrid}
4	7	0,571429	0,571429
11	15	0,733333	0,733333
26	31	0,83871	0,83871
57	63	0,904762	0,904762
120	127	0,944882	0,944882
247	255	0,968627	0,968627
502	511	0,982387	0,982387
1013	1023	0,990225	0,990225
2036	2047	0,994626	0,994626
4083	4095	0,99707	0,99707
8178	8191	0,998413	0,998413

The relative transmission speed allows you to understand which part of the key is used for information processing, and which part is used for additional operations to ensure the security and reliability of the cryptographic process. From the data in Table 1, it can be seen that $E_{McEliece}$ and E_{Hybrid} are inferior to E_{RSA} due to the redundancy associated with the use of error correction codes. However, as the size of the plaintext k increases, the efficiency can increase, since the control characters occupy a relatively smaller share of the total volume of transmitted data.

Figure 2 illustrates the data obtained as a result of studies of the relative speed of data transmission at different lengths of input and output messages for different encryption

algorithms, while for McEliece and hybrid systems, the condition was taken into account $2^r \leq k + r + 1$.

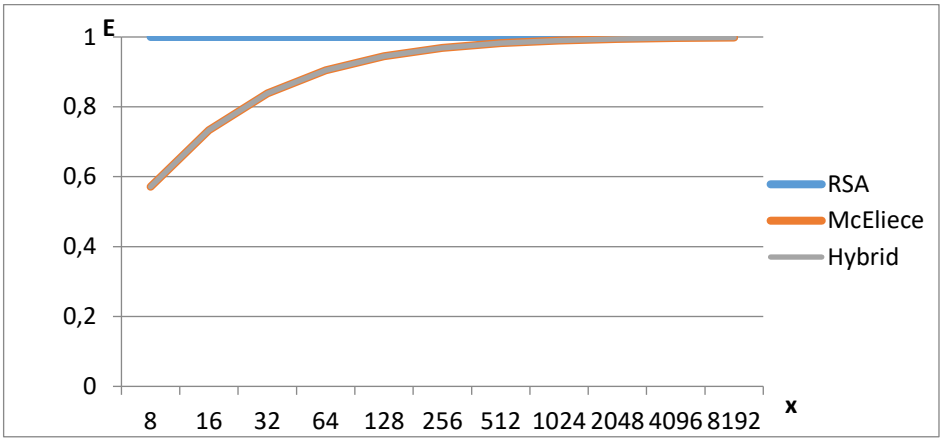

Fig. 2. Change in the relative speed of information transfer when the size of the message changes.

From the obtained data, it is evident that both for the McEliece system and the hybrid system, the relative data transmission speed increases with the size of the message. This means that the larger the amount of data to be transmitted, the closer the efficiency approaches 1, which is a desirable property of a cryptographic system.

The key size is a critical parameter that affects cryptographic strength, computational speed, memory usage, bandwidth, energy consumption, and key storage security. Balancing these aspects is important when choosing the optimal key size for a specific application. Key parameters in McEliece depend on the parameters of the code used, such as the number of rows r and the number of columns k of the generator matrix G', as well as the size of the elements in this matrix.

$$L_{McEliece} = r \times k \times log_2(n),$$

where n is the size of the field in which the elements of the matrix G' are defined, in particular for classical McEliece n=2 for binary fields.

The size of an RSA key is typically determined by the length of the modulus n in bits, which is obtained by multiplying two prime numbers p and q:

$$L_{RSA} = log_2(p \times q).$$

In Table 2, data is provided demonstrating the size of key data L for transmitting data m = 4 symbols at various field sizes n.

Table 2

Size of keys

n	$L_{McElice}$	L_{RSA}	L_{Hybrid}
35	28	6	174
221	28	8	232
899	28	10	290
1517	28	11	319
7387	28	13	377
10403	28	14	406
145157	28	18	522
826277	28	20	580

The analysis showed that the size of the McEliece key does not depend on the value of n, it remains constant at 28 bits. The size of RSA key data increases with n to ensure necessary cryptographic strength. The hybrid system combines elements of McEliece and RSA, explaining the increase in key size. This indicates that the system adapts to changes in

n, providing corresponding cryptographic resilience.

Figure 3 shows graphs depicting changes in the key size of the cryptographic system for encrypting the output message *m*=4 depending on *n*.

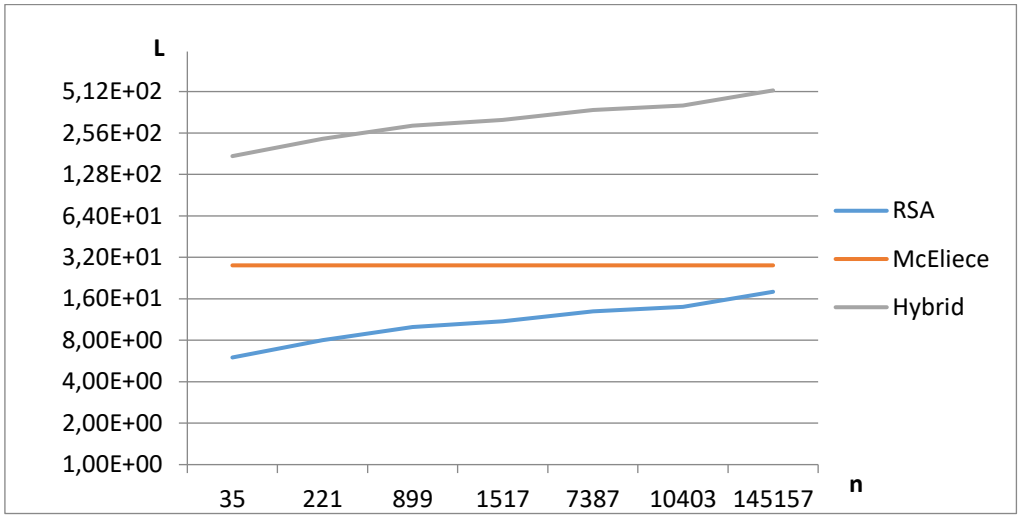

Fig. 3. Key Size Variation.

Increasing the field size *n* leads to an increase in key length for the RSA and hybrid cryptosystems, which indicates a higher level of security since larger keys make cryptanalysis more difficult. The constant key length of McEliece indicates limited adaptability of the classic McEliece algorithm to changes in field size. The hybrid cryptosystem demonstrates greater flexibility and adaptability to changes in field size, which can be beneficial in environments where security is critical. It offers a balanced solution, providing enhanced cryptographic resistance by increasing key size, but it requires more resources for computation and key storage.

The security of the hybrid cryptosystem is determined by the security of each of its components. To perform cryptanalysis of such a system, one needs to attack both McEliece and RSA. The most effective algorithms for this are Grover's algorithm [22], which can be used to attack the McEliece cryptosystem by searching for function roots or decoding sets, and Shor's algorithm [23], a quantum algorithm that allows for efficient factorization of numbers in the case of RSA.

The McEliece system is based on the use of error-correcting codes. Grover's algorithm can accelerate the search for an element in an unordered set, reducing the complexity from exponential $O(2^n)$ to $O(2^{n/2})$ due to quadratic speedup. This means that the complexity of the attack

$$T_{McEliece} = O\left(2^{\frac{2}{n}}\right)$$

will be significantly reduced, but still remains very high, making McEliece secure with large key sizes.

The security of RSA largely relies on the computational difficulty of factoring the number n for classical computers. Shor's algorithm can factorize n into prime factors in $O((log\ n)^3)$, which makes RSA vulnerable to quantum computers. To assess the resistance of RSA to attack

$$T_{RSA} = O((\log n)^3),$$

one can use the polynomial complexity of Shor's algorithm for factorization.

The resistance of the hybrid cryptosystem to quantum attacks can be evaluated as a combination of the resistance of each component:

$$T_{\text{Hybrid}} = T_{\text{McEliece}} + T_{RSA}$$
$$T_{\text{Hybrid}} = O((log\ n)^3) + O(2^{n/2}).$$

To decrypt a message in the hybrid cryptosystem, it is necessary to attack both components, as each performs different functions in the encryption process. First, the message needs to be decoded to remove the code redundancy introduced by the McEliece scheme, and then the result is decrypted using RSA to obtain the original message.

Table 3 presents the assessment of the cryptographic strength T of the systems for encrypting source data $m = 4$ characters at different values of n.

Table 3

Cryptographic Strength of Cryptosystems Against Attacks

n	$T_{McEliece}$	T_{RSA}	T_{Hybrid}
35	1,638E+04	1,349E+02	1,547E+26
221	1,638E+04	4,723E+02	8,308E+34
899	1,638E+04	9,447E+02	4,460E+43
1517	1,638E+04	1,180E+03	1,033E+48
7387	1,638E+04	2,122E+03	5,548E+56
10403	1,638E+04	2,376E+03	1,286E+61
145157	1,638E+04	5,042E+03	3,705E+78
826277	1,638E+04	7,595E+03	1,989E+87

The security of McEliece remains constant at 1.638E+04 regardless of the value of n, indicating the invariability of the key size. For the RSA system, the security increases with the increase in n, reflecting the dependency of RSA's strength on the size of the modulus. The hybrid system demonstrates the highest security, achieved by combining both systems.

Figure 4 shows the graphs of the cryptosystems' resistance to quantum attacks.

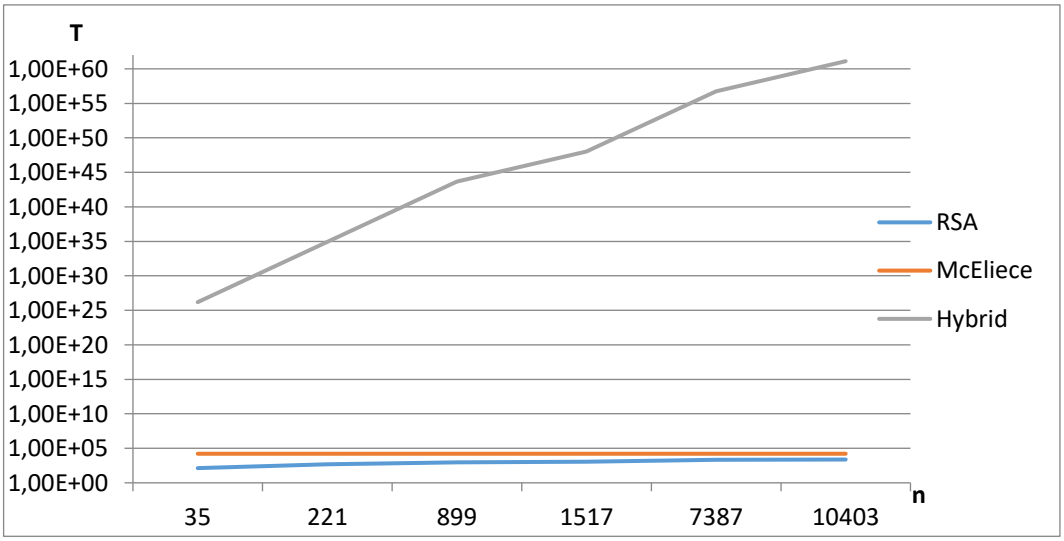

Fig. 4. Cryptosystem security as a function of n.

The hybrid cryptosystem demonstrates significantly higher cryptographic strength with increasing key size n compared to each algorithm individually. The combination of the effects of both systems allows achieving a high level of protection.

Conclusions. Both systems, McEliece and RSA, have a long history of scientific research and applications. Their cryptographic strength is based on different mathematical problems: McEliece relies on coding theory and combinatorial theory, while RSA relies on number theory and factorization. Combining them through the shared use of the value n does not contradict the mathematical principles and capabilities of both systems and also simplifies cryptographic key management.

These cryptosystems are known for their high resistance to various cryptanalytic attacks. Their integration allows for an increase in the key space by n times and complicates

approaches to breaking the ciphertext. RSA is used for encrypting short messages and digital signatures, while McEliece works well for long messages and is highly efficient in handling error correction codes. Integrating these systems allows for combining their advantages to ensure comprehensive information protection.

The conducted studies reflect important aspects of the efficiency of the proposed hybrid asymmetric cryptosystem based on codes. As the message size increases, the efficiency of data transmission increases, which is an important aspect for ensuring the speed of information exchange.

The increase in cryptographic strength of the proposed system with the increase in the Galois field size compared to the classic McEliece cryptosystem underscores the importance of the key length in cryptographic systems and their ability to protect information from cryptanalytic attacks. Specifically, increasing the key size by 6 times results in a 9.445×10^{21} times higher cryptographic strength, while changing the key data by 20 times results in a 1.214×10^{83} times higher strength. This emphasizes the importance of key length in relevant cryptographic systems and their ability to protect information from cracking attacks. The proposed hybrid cryptosystem allows for significantly improving data security by combining the advantages of both systems: McEliece provides the basic level of encryption and error correction, and the additional RSA protection enhances the overall resistance to $O\left(2^{n/2}\right) + O((log\ n)^3)$.

References

1. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signature and Public-Key Cryptosystems, *Communications of the ACM*. 1978. Vol. 21, No. 2. P. 120-126.
2. Khan M., Kamal U., Alam M., Khan H., Siddiqui S., Haque M., Parashar J. Analysis of Elliptic Curve Cryptography & RSA. *Journal of ICT Standardizatio.* 2023. Vol. 11_4. P. 355–378. doi: 10.13052/jicts2245-800X.1142.
3. Tchórzewski J., Jakóbik A. Theoretical and Experimental Analysis of Cryptographic Hash Functions. *Journal of Telecommunications and Information Technology*. 2019. Vol. 1. P.125-133. doi: 10.26636/jtit.2019.128018.
4. Amirkhanova D.S., Iavich M., Mamyrbayev O., Mamyrbayev O.Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles. *Cryptography. 2024.* Vol. 8, no. 3: 31. https://doi.org/10.3390/cryptography8030031.
5. Narwal E., Redhu Ritu. Mapping the Evolution of Code-Based Cryptosystems: A Comprehensive Analysis Using Science Mapping Techniques. 2024. doi: 10.9734/bpi/cpstr/v6/7513C.
6. González de la Torre M.A., Hernández Encinas L., Sánchez García J.I. Structural analysis of code-based algorithms of the NIST post-quantum call. *Logic Journal of the IGPL*. 2024. jzae071, doi: 10.1093/jigpal/jzae071.
7. Seck Boly., Cayrel P.-L., Diop I., Dragoi V.-F., Couzon K., Colombier B., Grosso V. Key-Recovery by Side-Channel Information on the Matrix-Vector Product in Code-Based Cryptosystems. *Information Security and Cryptology - ICISC 2022*. 2023. P.219-234. doi: 10.1007/978-3-031-29371-9_11.
8. Weger V., Gassner N., Rosenthal J. A Survey on Code-Based Cryptography. 2024.168 p. URL: https://arxiv.org/pdf/2201.07119.
9. Silva-García V.M., Flores-Carapia R., Alejandro Cardona-López M. A Hybrid Cryptosystem Incorporating a New Algorithm for Improved Entropy. *Entropy*. 2024. Vol. 26, no. 2. P. 154. doi: 10.3390/e26020154.
10. Suhael S., Ahmed Z., Hussain A. Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem. *Baghdad Science Journal*. 2023. doi: 10.21123/bsj.2023.8361.
11. Garms L., Paraïso T., Hanley N., Khalid A., Rafferty C., Grant J., Newman J., Shields A., Cid C., O'Neill M. Experimental Integration of Quantum Key Distribution and Post-

Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Advanced Quantum Technologies*. 2024. Vol. 7. doi: 10.1002/qute.202300304.

12. McEliece, R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report*. 1978. Vol. 42(44). P. 114-116.
13. Couvreur A., Mora R., Tillich J.-P. A New Approach Based on Quadratic Forms to Attack the McEliece Cryptosystem. 2023. doi: 10.1007/978-981-99-8730-6_1.
14. Lau T., Tan C.H. On the design and security of Lee metric McEliece cryptosystems. *Designs, Codes and Cryptography.* 2022. Vol. 90. doi:10.1007/s10623-021-01002-2.
15. Bindal E., Singh A. Secure and Compact: A New Variant of McEliece Cryptosystem. *IEEE Access*. 2024. P. 1-1. doi:10.1109/ACCESS.2024.3373314.
16. Parashar A. Enhanced McEliece Algorithm for Post-Quantum Cryptosystems. 2024. doi: 10.13140/RG.2.2.22002.93125.
17. Mariot L., Picek S., Yorgov, R. On McEliece-Type Cryptosystems Using Self-Dual Codes With Large Minimum Weight. *IEEE Access*. 2023. P. 1-1. doi: 10.1109/ACCESS.2023.3271767.
18. Anuradha M., Loganathan S., Suseela G., Selvan M.P., Nalini M., Chitra D.D, Hybrid Multiple Cryptography for Data Encryption. *2023 8th International Conference on Communication and Electronics Systems (ICCES)*. 2023. P. 596-603. doi: 10.1109/ICCES57224.2023.10192838.
19. Jintcharadze E., Iavich M. Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. *2020 IEEE East-West Design & Test Symposium (EWDTS)*. 2020. P. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.
20. Jian M.-S., Cheng Y.-E., Shen C.-H. Internet Of Things (IOT) Cybersecurity based on the Hybrid Cryptosystem. *2019 21st International Conference on Advanced Communication Technology (ICACT)*. 2019.P. 176-181, doi: 10.23919/ICACT.2019.8701957.
21. Кузнецов О.О., Горбенко Ю.І., Кіян А.С., Уварова А.О., Кузнецова Т.Ю.Порівняльні дослідження та аналіз ефективності гібридної кодовоїкриптосистеми. Радіотехніка. 2018. Вип. 195. С. 61-69.
22. Opiłka F., Niemiec M., Gagliardi M., Kourtis M. A., 2024. Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature. *Applied Sciences*. 2024. Vol. 14, no. 12: 4994. doi: 10.3390/app14124994.
23. Regev, Oded. An Efficient Quantum Factoring Algorithm. 2023. URL: https://arxiv.org/pdf/2308.06572.

ГІБРИДНА АСИМЕТРИЧНА КРИПТОСИСТЕМА НА ОСНОВІ КОДІВ

А.Я. Давлетова

Західноукраїнський національний університет,
11, Львівська вул., м.Тернопіль, 46020, Україна;
email: a7davletova@gmail.com

Робота присвячена вирішенню актуальної задачі забезпечення надійного захисту інформації в умовах збільшення обсягів даних та зростання кількості кіберзагроз. Традиційні криптографічні системи, хоча і є досить надійними, можуть виявитися вразливими до нових типів атак, особливо до квантових. Це підкреслює необхідність пошуку та дослідження більш стійких методів шифрування. У роботі запропонована гібридна криптосистема, що поєднує систему McEliece та алгоритм шифрування RSA. Такий підхід дозволяє використати переваги обох методів: високий рівень безпеки RSA, заснований на складності факторизації великих чисел, та стійкість McEliece до квантових атак завдяки складності декодування довільних лінійних кодів. Особливістю запропонованої гібридної системи є використання полів Галуа *GF(p)* для всіх операцій, що забезпечує додатковий рівень захисту та гнучкість. Інтеграція асиметричних криптоалгоритмів, стійкість яких базується на вирішенні різних математичних задач, забезпечує підвищення надійності та безпеки запропонованої системи. Використання спільного параметра n для генерації ключів також спрощує управління ними та розширює словник у n разів. Таке рішення поєднує в собі захист від помилок та криптографічну безпеку, що робить його потужним інструментом для захисту даних в умовах обміну інформацією через потенційно ненадійні канали передачі. Дослідження, проведені в рамках роботи, спрямовані на аналіз ефективності та безпеки запропонованої гібридної криптосистеми. Особлива увага приділена таким характеристикам, як відносна швидкість передачі інформації, довжина шифротексту, обсяг ключів та стійкість до криптоаналізу. Результати демонструють переваги гібридної системи у порівнянні із використанням кожного з алгоритмів окремо.

Ключові слова: криптосистема McEliece, алгоритм шифрування RSA, скінчені поля Галуа, гібридна криптосистема, стійкість до криптоаналізу.