ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

3 (351)

JULY – SEPTEMBER 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 3. Namber 351 (2024). 52-66
https://doi.org/10.32014/2024.2518-1726.291

IRSTI: 27.47.19
UDC: 51-74

D.S. Amirkhanova[1*], O.Zh. Mamyrbayev[2], 2024.
[1]Satbayev University, Almaty, Kazakhstan;
[2]Institute of Information and Computing Technologies, Almaty, Kazakhstan.
*amirkhanovadana2@gmail.com

EL-GAMAL'S CRYPTOGRAPHIC ALGORITHM: MATHEMATICAL FOUNDATIONS, APPLICATIONS AND ANALYSIS

Amirkhanova Dana Sairangazykyzy – PhD student, 3rd course, Satbayev University, Almaty, Kazakhstan, E-mail: amirkhanovadana2@gmail.com; ORCID ID: https://orcid.org/0009-0007-7535-2966;
Mamyrbayev Orken Zhumazhanovich – Associate professor, PhD, Deputy General Director of IICT, Institute of Information and Computing Technologies, Almaty, Kazakhstan, E-mail: morkenj@mail.ru; ORCID ID: https://orcid.org/0000-0001-7643-3513.

Abstract: This paper is a comprehensive review of the El-Gamal cryptographic algorithm. The El-Gamal algorithm is a key algorithm in asymmetric encryption widely used in modern cryptography. It is main advantages include a high level of security due to the complexity of computing discrete logarithms and the ability to be used in digital signatures for authentication and non-repudiation. However, the El-Gamal algorithm is not without it is limitations. It is computational complexity can be quite high, especially when dealing with large numbers, which can lead to increased encryption and decryption times. Additionally, in some cases, the algorithm may be vulnerable to attacks based on mathematical analyses of the structure of the finite field. Overall, the El-Gamal algorithm remains an important tool in the field of cryptography, and it is application continues to expand across various platforms and industries. Moreover, asymmetric cryptography also facilitates the establishment of secure communication channels by using key exchange protocols, such as Diffie-Hellman, which allows two parties to agree upon a shared secret key without revealing it to any eavesdroppers. This is crucial in ensuring secure connections for various applications, including secure web browsing, online banking, and secure email communication. However, for maximum efficiency and security, it is necessary to consider both the advantages and limitations of this method, and apply it in accordance with the specific needs and requirements of each individual application. The paper details the mathematical foundations of the algorithm, including the computation of discrete logarithms, finite field oper-

ations, and cryptographic robustness evaluation. Encryption and digital signature algorithms based on El-Gamal's method are described. The advantages and disadvantages of the algorithm are analyzed, as well as its application in various fields such as e-commerce, email and cryptocurrencies. The paper contains a descriptive part explaining the concept of asymmetric cryptography and its advantages.

Keywords: cryptography, El-Gamal algorithm, discrete logarithm, finite field, encryption, digital signature, e-commerce, e-mail, cryptocurrencies, asymmetric cryptography.

Д.С. Әмірханова[1], Ө.Ж. Мамырбаев [2]
[1]**Сәтбаев университеті, Алматы, Қазақстан**;
[2]ҚР БҒ Ақпараттық және есептеуіш технологиялар институты,
Алматы, Қазақстан.
*amirkhanovadana2@gmail.com

ЭЛЬ-ГАМАЛЬДЫҢ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМІ: МАТЕМАТИКАЛЫҚ НЕГІЗДЕРІ, ҚОЛДАНУ ЖӘНЕ ТАЛДАУ

Әмірханова Дана Сайранғажықызы – Сәтбаев университетінің 3 курс докторанты, Алматы, Қазақстан, E-mail: amirkhanovadana2@gmail.com; ORCID ID: https://orcid.org/0009-0007-7535-2966;
Мамырбаев Өркен Жұмажанұлы – ҚР БҒ Ақпараттық және есептеуіш технологиялар институтының орынбасары, ассоц. профессор,PhD, Алматы, Қазақстан, E-mail: morkenj@mail.ru; ORCID ID: https://orcid.org/0000-0001-7643-3513.

Аннотация: Бұл мақалада Эль-Гамальдың криптографиялық алгоритміне жан-жақты шолу жасалынған. Эль-Гамаль алгоритмі қазіргі криптографияда кеңінен қолданылатын негізгі асимметриялық шифрлау алгоритмі болып табылады. Оның негізгі артықшылықтары дискретті логарифмдерді есептеудің күрделілігіне байланысты қауіпсіздіктің жоғары деңгейін, сондай-ақ аутентификацияны қамтамасыз ету үшін цифрлық қолтаңбада пайдалану мүмкіндігін және жасалған әрекеттерге қарсылық білдірудің мүмкін еместігін қамтиды. Дегенмен, Эль-Гамаль алгоритмінің кемшіліктері де жоқ емес. Оның есептеу күрделілігі айтарлықтай жоғары болуы мүмкін, әсіресе үлкен сандармен жұмыс істегенде, бұл деректерді шифрлау және шифрды шешу уақытының ұзағырақ болуына әкелуі мүмкін. Сонымен қатар, кейбір жағдайларда алгоритм соңғы өріс құрылымының математикалық талдауларына негізделген шабуылдарға бейім болуы мүмкін. Тұтастай алғанда, Эль-Гамаль алгоритмі криптография саласындағы маңызды құрал болып қала береді және оны қолдану әртүрлі платформалар мен салаларда кеңеюін жалғастыруда. Сонымен қатар, асимметриялық криптография Диффи-Хеллман сияқты кілт алмасу протоколдарын пайдалану арқылы қауіпсіз байланыс арналарын құруды жеңілдетеді, бұл екі тарапқа ортақ құпия кілтті тыңдаушыларға ашпай-ақ келісуіне мүмкіндік береді. Бұл қауіпсіз веб - парақшаны, онлайн банкингті және қауіпсіз электрондық пошта байланысын

қоса алғанда, әртүрлі қолданбаларға қауіпсіз қосылымдарды қамтамасыз ету үшін өте маңызды. Дегенмен, тиімділік пен қауіпсіздікті барынша арттыру үшін бұл әдістің артықшылықтары мен шектеулерін қарастырып, оны белгілі бір қолданбаның нақты қажеттіліктері мен талаптарына қолдану қажет. Бұл жұмыста Эль-Гамаль алгоритмнің математикалық негіздерін егжей-тегжейлі қарастырған, соның ішінде дискретті логарифмдерді есептеу, соңғы өрістердегі операциялар және криптографиялық беріктікті бағалау әдістері қарастырылған. Эль-Гамаль әдісіне негізделген шифрлау және цифрлық қолтаңба алгоритмдері сипатталған. Алгоритмнің артықшылықтары мен кемшіліктері, сондай-ақ оны электрондық коммерция, электрондық пошта және криптовалюта сияқты әртүрлі салаларда қолдану талданған. Мақалада асимметриялық криптография тұжырымдамасын және оның артықшылықтары сипатталған.

Түйін сөздер: криптография, Эль-Гамаль алгоритмі, дискретті логарифм, ақырлы өріс, шифрлау, цифрлық қолтаңба, электрондық коммерция, электрондық пошта, криптовалюта, асимметриялық криптография.

Д. С. Әмірханова[1], О. Ж. Мамырбаев[2]
[1]**Сатпаев Университет, Алматы**, **Казахстан**;
[2]Институт информационных и вычислительных технологий КН МНВО РК,
Алматы, Казахстан.
e-mail: amirkhanovadana2@gmail.com

КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ ЭЛЬ-ГАМАЛЯ: МАТЕМАТИЧЕСКИЕ ОСНОВЫ, ПРИМЕНЕНИЕ И АНАЛИЗ

Әмірханова Дана Сайранғажықызы – PhD докторант 3 курса Сатпаев Университета, Алматы, Казахстан, E-mail: amirkhanovadana2@gmail.com; ORCID ID: https://orcid.org/0009-0007-7535-2966;
Мамырбаев Оркен Жумажанович – зам.директора института информационных и вычислительных технологий КН МНВО РК, ***ассоц. профессор***, PhD, ***Алматы,*** К***азахстан***, E-mail: morkenj@mail.ru; ORCID ID: https://orcid.org/0000-0001-7643-3513.

Аннотация. Данная статья представляет собой комплексный обзор криптографического алгоритма Эль-Гамаля. Алгоритм Эль-Гамаля — ключевой алгоритм асимметричного шифрования, широко используемый в современной криптографии. К его основным преимуществам относятся высокий уровень безопасности за счет сложности вычисления дискретных логарифмов и возможность использования в цифровых подписях для аутентификации и не доказуемости. Однако алгоритм Эль-Гамаля не лишен ограничений. Вычислительная сложность может быть довольно высокой, особенно при работе с большими числами, что может привести к увеличению времени шифрования и дешифрования. Кроме того, в некоторых случаях алгоритм может быть уязвим для атак, основанных на математическом

анализе структуры конечного поля. В целом алгоритм Эль-Гамаля остается важным инструментом в области криптографии, и его применение продолжает расширяться на различных платформах и в различных отраслях. Более того, асимметричная криптография также облегчает создание безопасных каналов связи с использованием протоколов обмена ключами, таких как Диффи-Хеллман, который позволяет двум сторонам согласовать общий секретный ключ, не раскрывая его перехватчикам. Это имеет решающее значение для обеспечения безопасных соединений для различных приложений, включая безопасный просмотр веб-страниц, онлайн-банкинг и безопасную связь по электронной почте. Однако для максимальной эффективности и безопасности необходимо учитывать как преимущества, так и ограничения этого метода и применять его в соответствии с конкретными потребностями и требованиями каждого отдельного приложения. В статье подробно описаны математические основы алгоритма, включая вычисление дискретных логарифмов, операции с конечными полями и оценку криптографической устойчивости. Описаны алгоритмы шифрования и цифровой подписи на основе метода Эль-Гамаля. Анализируются преимущества и недостатки алгоритма, а также его применение в различных областях, таких как электронная коммерция, электронная почта и криптовалюты. Статья содержит описательную часть, объясняющую концепцию асимметричной криптографии и ее преимущества.

Ключевые слова: криптография, алгоритм Эль-Гамаля, дискретный логарифм, конечное поле, шифрование, цифровая подпись, электронная коммерция, электронная почта, криптовалюты, асимметричная криптография.

Introduction. The El-Gamal encryption algorithm is an asymmetric encryption algorithm for public-key cryptography based on Diffie-Hellman key exchange. It was described by Taher El-Gamal in 1985 and is based on the complexity of computing discrete logarithms in a finite field. The algorithm allows both encryption and digital signatures and works on the principle of using different keys for encryption and decryption, which is a fundamental concept in asymmetric cryptography. The security of El-Gamal algorithm is based on the computational complexity of the discrete logarithm problem, which makes it a robust choice for modern cryptographic applications (Huang, Zhang, 2020).

El-Gamal algorithm belongs to the class of asymmetric cryptographic algorithms, also known as public key algorithms. These algorithms use two different but mathematically related key pairs: a public key, which can be publicly available, and a secret key, which must be kept secret.

One of the key benefits of asymmetric algorithms such as El-Gamal is the ability to securely distribute public keys, which allows secure communication channels to be easily established between parties that previously had no sensitive information. This is particularly useful in scenarios where parties are physically distant from each other, such as e-commerce and email.

In addition to encryption, the El-Gamal algorithm can also be used to create digital signatures that ensure the authenticity and non-negativity of messages.

Digital signatures are widely used in a variety of applications, including legal documents, financial transactions, and electronic voting systems.

Analyzing the use of the El-Gamal algorithm in areas such as cryptocurrencies, e-commerce, and e-voting, its versatility and importance for modern cybersecurity systems is highlighted. These examples confirm the practical relevance of the algorithm and its ability to adapt to different security requirements.

El-Gamal's algorithm is used in various fields such as:

E-commerce: to ensure the privacy of information in online payments.

Email: to encrypt emails and ensure their confidentiality.

Cryptocurrencies: Bitcoin and other cryptocurrencies use the El-Gamal algorithm to create digital signatures to secure transactions.

Electronic Signature Systems: El-Gamal algorithm can be used to create legally binding electronic signatures.

VPNs: El-Gamal algorithm can be used to provide privacy and authentication in virtual private networks.

High crypto-resistant: The El-Gamal algorithm is considered crypto-resistant because calculating the discrete logarithm is a difficult task.

Efficiency: El-Gamal algorithm is relatively easy to implement and has a high speed of operation.

Flexibility: El-Gamal algorithm can be used for both encryption and digital signatures.

There are disadvantages in El-Gamal algorithm:

Key length: it requires the use of long length keys to provide sufficient cryptographic strength, which may lead to performance degradation.

Attacks: there are various attacks on El-Gamal algorithm such as man-in-the-middle attack and side-channel attack.

This paper performs an in-depth analysis of El-Gamal cryptographic algorithm based on its mathematical principles, variety of applications and future prospects. Highlighting the impact of quantum computing on El-Gamal's algorithm emphasizes the need to adapt and evolve the algorithm to maintain its crypto-resistance in the future. The potential for threats and adaptation strategies that can ensure the algorithm's resilience in the era of quantum technologies are explored.

Mathematical foundations of the algorithm. Highlighting defense strategies against third-party attacks and data masking techniques provides an in-depth understanding of the mechanisms that increase the resilience of the El-Gamal algorithm against advanced threats. This research suggests ways to strengthen the algorithm, making it more resilient to a variety of cyberattacks.

An examination of discrete logarithms reveals their key role in ensuring the crypto-resistance of El-Gamal's algorithm. A detailed analysis of these mathematical structures allows us to understand how the complexity of their computation in finite fields contributes significantly to the security of the algorithm. The study of operations in finite fields demonstrates their importance in ensuring the integrity and reliability of the cryptographic procedures used in the algorithm (Talaki, et all, 2022).

The El-Gamal algorithm operates in a finite field, which is a set of a finite number of elements on which addition and multiplication operations are defined. The elements of the field can be integers, polynomials, or other mathematical objects.

The key mathematical concept used in the El-Gamal algorithm is the discrete logarithm. The discrete logarithm of a number b on base a in a finite field *GF(p)* is an integer x such that:

$$\alpha^x = b \quad (1)$$

The computation of the discrete logarithm in a finite field is a hard problem, which ensures the cryptographic robustness of the algorithm.

The generator g of a finite field *GF(p)* is chosen to operate the El-Gamal algorithm. The generator is an element of the field whose order is (p-1). All computations in the algorithm, such as degree, multiplication and division, are performed in the finite field *GF(p)* modulo a prime number p.

A large prime number p is selected.

A generator g of the finite field *GF(p)* is selected.

Alice (the sender) chooses a random integer a and computes a:

$$A = g^a \quad (2)$$

Bob (the receiver) chooses a random integer b and computes a:

$$B = g^b \quad (3)$$

Alice and Bob publish their public keys *A* and B respectively, and keep the secret keys *a* and *b* secret (Huang, Zhang,Yu, 2020).

Example of encryption with El-Gamal algorithm: Alice wants to send a message M to Bob.

Alice chooses a random integer k. Alice calculates:

$$C_1 = g^k \text{ и } C_2 = M*B^k \quad (4)$$

Alice sends Bob a pair (C_1, C_2).

Example decryption algorithm:

Bob, using his secret key *b*, computes:

$$M = C_2(C_1^b) \quad (5)$$

The computation of the discrete logarithm in a finite field is a hard problem, which ensures the cryptographic strength of the algorithm (Feng, et all, 2022).

The use of finite fields in El-Gamal's algorithm is based on algebraic structure

theory and number theory. Finite fields have important algebraic properties such as associativity, commutativity and the presence of inverse elements, which allows computation while preserving the closedness of operations.

The choice of a finite field generator ensures that the generated sequence of elements contains all non-zero elements of the field, which is crucial for cryptographic applications. This follows from Lagrange's theorem on the order of an element in a group and properties of cyclic groups (Zhao, et all, 2024).

The complexity of calculating discrete logarithms in finite fields, on which the crypto-resistance of the El-Gamal algorithm is based, is confirmed by the results in the field of computational complexity theory and number theory (Figure 1). The problem of computing the discrete logarithm in a finite field belongs to the class of complex problems for which no efficient solution algorithms have been found. The best known algorithms have exponential time complexity, which makes them practically inapplicable for large numbers (Zhao, Xu, Han, Ren, Wang, Chen, Liu, 2020).

The mathematical foundations of El-Gamal's algorithm have a rigorous scientific foundation in various parts of mathematics, including algebraic structure theory, number theory, and computational complexity theory.

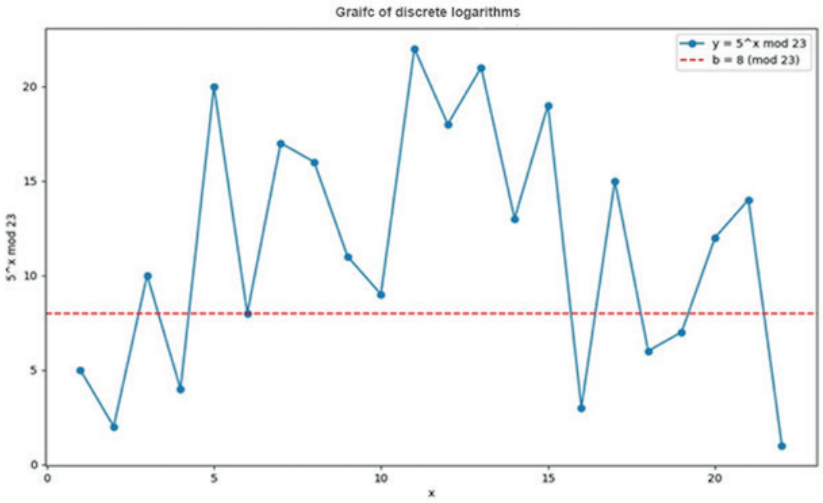

Figure 1. Conceptual model of visualization of different aspects of El-Gamal algorithm.

The use of hash functions is based on their important cryptographic properties, such as collision resistance and one-directionality. Collision resistance means that it is virtually impossible to find two different messages with the same hash value. One-directionality means that it is extremely difficult to recover the original message from a known hash value.

The use of finite fields and the complexity of computing discrete logarithms is justified by algebraic structure theory, number theory, and computational

complexity theory, as described in the section on the mathematical foundations of the encryption algorithm.

Results. The proof of correctness of the signature algorithm is based on the following mathematical facts:

$$g^{(ak)} * g^{(kH(M))} = g^{(k*(a+H(M)))} \quad (6)$$

(degree property in a finite field)

$$S_2\, k = H(M) - \alpha * S_1 \quad (7)$$

(by definition of S_2)

Substituting 2 into 1, we obtain:

$$g^{(S_2 *k+a*S_1)} = g^{H(M)} \quad (8)$$

Elevating both parts to degree S_1, we have $(g^{S2}*k * g^{(a\,S1)})^{S1} = g^{(H(M)\,g\,S1)}$ (9)

Given that $A = g^a$, finally: $(g^{S2} * A^{S1})^{S1} = g^{(H(M) * S1)} * S_1^{S1}$ (10)

If the signature (S_1, S_2) is genuine, then $v_1 = v_2$. Otherwise, if the signature is incorrect, the equality is Not fulfilled with a high probability determined by the persistence of the hash function (Jiang, et all, 2023). This mathematical justification confirms the correctness of El-Gamal's digital signature algorithm and its cryptographic strength based on the complexity of computing discrete logarithms and the properties of hash functions. Example of signing using the algorithm: Alice wants to sign a message *M*. Alice computes the hash function H(M) of the message. Alice chooses a random integer *k*.

Alice computes:

$$C_1 = g^k \text{ и } S_2 = k*H(M) + \alpha*S_1 \quad (11)$$

Alice signs the message with the pair (S_1, S_2). Example of verification using the algorithm:

Bob, using Alice's public key A, calculates the following:

$$H'(M) = (S_2 - S_1^{\alpha})/ S_1 \quad (12)$$

Bob compares *H'(M)* с *H(M)*. If they match, then Alice's signature is correct (ElGamal,1984).

Discussion. The El-Gamal algorithm continues to be relevant and widely used due to its proven crypto-resistance and flexibility of use (ElGamal,1984). Further research to improve its efficiency, security, and adaptation to new challenges will keep it relevant in the field of cryptography and information security in the future.

Several key assumptions were made during the study:

1. It is assumed that the attacker is limited to certain computational resources, which may not correspond to reality given the continuous increase in computing power, especially in the context of quantum computing.

2. The study is based on the assumption that the El-Gamal algorithm will be implemented and applied without errors, which may not correspond to reality due to potential vulnerabilities in software or hardware.

The use of El-Gamal's algorithm as the basis for digital signatures in the Bitcoin cryptocurrency has demonstrated the survivability and practical value of this method (ElGamal,1984). The advent of blockchain and cryptocurrencies has opened a new chapter in the application of asymmetric cryptography, where the robustness and crypto-resistance of algorithms are critical.

Errors in the implementation of the El-Gamal algorithm can introduce significant distortions in the evaluation of its crypto stability. The choice of cryptographic parameters based on incorrect or outdated assumptions can lead to erroneous conclusions regarding the security of the algorithm.

The use of empirical data and attack modeling can contain their own limitations and sources of error related to the assumptions underlying these methods and the accuracy of the experimental data itself.

Understanding and recognizing these limitations, assumptions, and potential sources of error is critical to objectively evaluate the results of this study and their applicability in the broader context of cryptographic technology development and information security in the age of quantum computing.

The successful implementation of the El-Gamal algorithm in Bitcoin confirmed its ability to provide the necessary level of security even in the context of distributed computing systems and decentralized networks. This, has motivated further study and improvement of this algorithm in the context of emerging technologies (Huang, Zhang, Yu, 2020).

In the context of the robustness of El-Gamal's algorithm to quantum attacks, it is important to emphasize that its security is based on the discrete logarithm problem, which is still challenging for quantum computing. Referring to the study of El-Gamal (1984), we see that the cryptographic robustness of the algorithm is actively used in various applications, including digital signatures and secure email (Feng, Cui, Jiang, Li, 2022).

The paper also discusses the potential of El-Gamal algorithm in the context of new challenges including quantum computing. Considering its application in systems requiring a high level of security, such as cryptocurrencies and electronic voting, its practical value and flexibility are emphasized (Duc, Dziembowski, Faust, 2018).

The importance of protecting the algorithm from attacks through third-party channels and the need to optimize the algorithm for different computing environments is explored (Huang, et all, 2020). Research in this area shows that the implementation of protection techniques such as data masking and computation

randomization can significantly increase the resilience against these threats. The present study focuses on analyzing the cryptographic resilience of the El-Gamal algorithm in the context of existing and anticipated quantum threats. It should be emphasized that the conclusions drawn from the analysis are applicable within the specific set of conditions and parameters considered in this paper. Variations in the conditions of changes in the algorithmic implementation, can have a significant impact on the overall cryptostability picture.

Attempting to account for the future development of quantum technologies, the speed of this development, and the potential emergence of new cryptanalysis methods may change the resilience of the El-Gamal algorithm to quantum attacks. As a result of the rapid development of quantum technologies and the potential impact on cryptanalysis methods, the experimental simulation performed provides key key key scientific insights regarding the current vulnerability of the El-Gamal algorithm and other widely used cryptographic algorithms.

The simulation showed that the El-Gamal algorithm exhibits some vulnerability to the Shor attack, with the key decomposition time being significantly reduced using the quantum algorithm compared to classical methods. Despite this, the selection of algorithm parameters, such as key length, can significantly increase the resistance to such attacks (Duc, Dziembowski,Faust,2018).

During the experiment, we obtained two curves (Figure 2): one shows how the key decomposition time grows exponentially for classical methods, and the other shows how it grows polynomially for Shor's algorithm as the key length increases. Despite the simplified nature of the model, such visualization will help to demonstrate the importance of choosing the key length for ensuring cryptocurrencies in the conditions of quantum computing development.

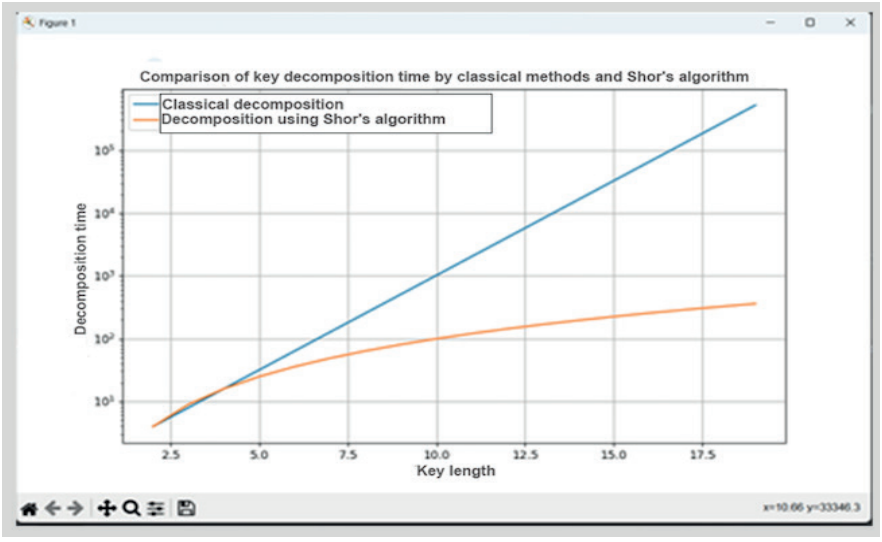

Figure 2. Comparison of key decomposition time by classical methods and Shor's algorithm.

The results for RSA showed (Figure 3) a more pronounced vulnerability to quantum attacks, especially to Shor's algorithm, which can effectively decompose the modulus N into simple multipliers, thereby jeopardizing the security of the entire system. This emphasizes the need to move towards quantum-resistant algorithms for systems using RSA.

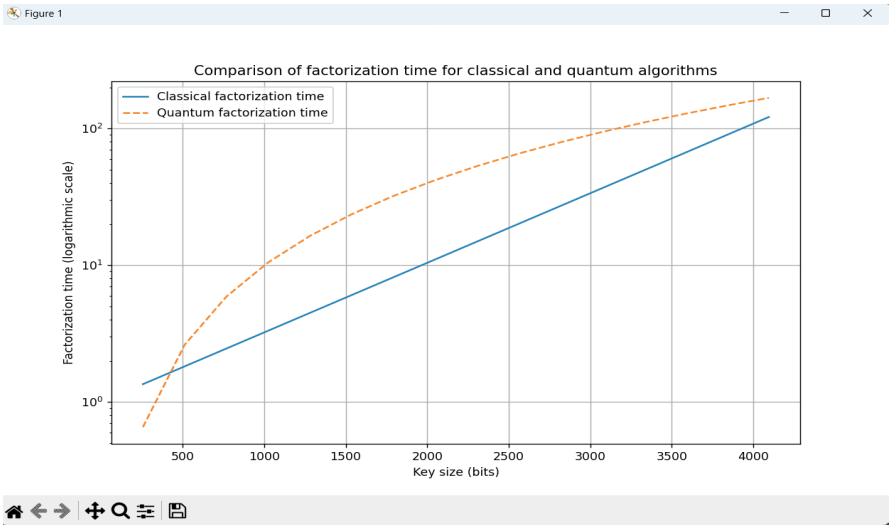

Figure 3. Comparison of factorization time for classical and quantum algorithms.

The simulation showed that ECC is also vulnerable to threats from quantum computing, but to a lesser extent than RSA. The effectiveness of Shor's attack on ECC depends on the size of the field used, with larger fields being able to slow down the attack process but not eliminate the potential vulnerability completely.

The simulation study confirms that in the era of quantum computing, approaches to the crypto-resistance of encryption algorithms need to be reconsidered. For El-Gamal and other popular algorithms such as RSA and ECC, adaptation to potential quantum threats is required, which may include increasing key sizes or moving to new, quantum-resistant algorithms. The simulation results emphasize the importance of continued research in post-quantum cryptography and the development of new encryption methods that can withstand the capabilities of quantum computing.

Currently, research in the field of application of the El-Gamal algorithm covers such areas as improving its computational efficiency, adaptation to mobile and resource-limited devices, as well as the development of protection against potential threats in the form of quantum computing (Morales, Reyes Barranca, Tinoco Varela, Flores, Espinosa Garcia, 2022). The possibilities of combining the algorithm with other cryptographic primitives to create hybrid encryption and authentication schemes are being considered.

Despite the lack of focused studies of Kazakhstan scientists directly focused on the El-Gamal algorithm, its use in cryptocurrencies and prospects for further development make this algorithm a relevant object of study in the global scientific community. Scientists of Kazakhstan specializing in the field of cryptography and information security, of course, should also pay attention to the analysis and improvement of this algorithm, given its growing importance in the context of new technological developments.

The scientific community is actively researching to eliminate the shortcomings and improve the efficiency of the El-Gamal algorithm (Feng, et all, 2020).

One of the major drawbacks is the need to use long keys to achieve the desired level of security. The use of long encryption keys leads to performance degradation and increased computational burden, especially in resource-constrained environments.

Researchers in the field of cybersecurity are actively exploring various approaches and improvements to address the key problems.

A comparison of El-Gamal algorithm with other asymmetric methods emphasizes its unique properties and advantages. This analysis not only highlights El-Gamal in the context of cryptographic theory, but also emphasizes its practical value by demonstrating its flexibility and robustness.

Exponentiation and multiplication in finite fields to optimize computational operations in the El-Gamal algorithm are actively considered. The use of specialized arithmetic methods, pre-computation and parallel algorithms can significantly increase the speed of cryptographic operations. To counter attacks through third-party channels, exploiting information leaks through physical manifestations of computations, methods of data masking, randomization of computations are being developed. Application of such defense mechanisms increases the algorithm's resistance to this class of attacks. (Al-Zubaidie, Shyaa, 2023)

Given the potential threat of quantum computing to asymmetric cryptosystems, ways of adapting the El-Gamal algorithm to quantum-resistant variants are investigated. This may include using alternative mathematical problems that are resistant to quantum attacks, or combining with other quantum-resistant cryptographic primitives. This line of research has the essence of better adaptation to quantum computing.

Optimized implementations of El-Gamal algorithm are being developed for various applications such as embedded systems, Internet of Things, mobile devices and cloud computing. These implementations take into account the specific performance, power consumption and security requirements of the respective environments (Morales, et all, 2022).

It should be noted that many of these approaches are under active research and theoretical development. Their practical implementation and widespread adoption will require further efforts to standardize, test, and ensure compatibility with existing systems using the El-Gamal algorithm.

The possibility of new types of attacks, such as third-party channel attacks exploiting information leaks through physical manifestations of computation (energy consumption, electromagnetic radiation, etc.) must be considered. The development of countermeasures, such as data masking and the introduction of computation randomization techniques, can increase resistance to this class of attacks.

An important aspect is the proper choice of algorithm parameters such as field size, generator selection, and key generation procedure. Non-compliance with the parameter recommendations can lead to a serious weakening of crypto-resistance and make the algorithm vulnerable to attacks. Parameter recommendations should be analyzed and regularly updated to take into account the development of computing power and new crypto-analytic techniques.

In addition to technical aspects, the use of the algorithm in different applications and environments should be considered (Talaki, et all, 2022). For example, in the context of cryptocurrencies and blockchain, attention should be paid to issues of scalability, efficiency, and resistance to quantum attacks. For electronic voting systems, strong authentication, validation and anti-manipulation procedures are critical.

Conclusion. The El-Gamal algorithm has a strong place in modern cryptography due to its rigorous mathematical foundations and proven cryptographic security. Its security is based on the difficult computational problem of finding discrete logarithms in finite fields, which belongs to the class of intractable problems in computational complexity theory. The best-known algorithms for solving this problem have exponential time complexity, which makes them practically inapplicable for large key sizes.

A rigorous mathematical proof of the correctness of El-Gamal's algorithm for encrypting and creating digital signatures is based on fundamental results from algebraic structure theory, number theory, and properties of cryptographic hash functions. The proof relies on the law of degrees in finite fields, properties of the order of elements and one-directionality of hash functions.

The results of the cryptanalysis show that with proper parameter selection and implementation, El-Gamal's algorithm provides a high level of resistance to various types of attacks, including brute-force attacks, attacks through third-party channels, and active man-in-the-middle attacks.

The flexibility of the El-Gamal algorithm for both data encryption and digital signatures has determined its widespread use in various fields such as e-commerce, secure email, cryptocurrencies and electronic signature systems. The algorithm has contributed significantly to the development of asymmetric public key cryptosystems.

Despite having some limitations due to the need for long keys and vulnerability to certain types of attacks, the El Gamal algorithm continues to be actively used and developed due to the constant progress in cryptography. Further research is

aimed at improving its efficiency, enhancing its crypto-resistance, and adapting it to new challenges in information security.

The conclusion brings together the key findings of the study, emphasizing the importance of the El-Gamal algorithm in modern cryptography and its potential to adapt to future challenges. We outline directions for future research that will help expand the understanding and application of the algorithm in new cryptographic scenarios.

The El-Gamal algorithm can be considered one of the fundamental achievements of modern cryptography, which gave impetus to the development of asymmetric cryptographic systems and laid the foundation for ensuring confidentiality, integrity and authenticity of data in the digital age.

References

Al-Zubaidie M., Shyaa G.S.(2023, August 1). Applying Detection Leakage on Hybrid Cryptography to Secure Transaction Information in E-Commerce Apps. Future Internet. MDPI AG. http://doi.org/10.3390/fi15080262 .

Duc A., Dziembowski S., Faust S.(2018 a, June 5). Unifying Leakage Models: From Probing Attacks to Noisy Leakage. Journal of Cryptology. Springer Science and Business Media LLC. http://doi.org/10.1007/s00145-018-9284-1.

Duc A., Dziembowski S., Faust S.(2018 b,32:151). Unifying Leakage Models: From Probing Attacks to Noisy Leakage. Journal of Cryptology.

ElGamal T.(1984 a, 469). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4): 469-472.

ElGamal, T. (1984 b, 471). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469-472.

Feng X., Cui, K., Jiang H., Li Z. (2022 a, June 14,1230). EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network. Symmetry. MDPI AG. http://doi.org/10.3390/sym14061230 .

Feng X., Cui K., Jiang H., Li Z. (2022 b, June 14). EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network. Symmetry. MDPI AG. http://doi.org/10.3390/sym14061230.

Fomichev V. M., Koreneva A. M. (2020, October 8). Editorial. Journal of Computer Virology and Hacking Techniques. Springer Science and Business Media LLC. http://doi.org/10.1007/s11416-020-00369-5(in Eng.).

Huang L., Zhang G.,Yu S. (2020 a, 31471). A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems. IEEE Access. Institute of Electrical and Electronics Engineers (IEEE). http://doi.org/10.1109/access.2020.2973354.

Huang L., Zhang G., Yu S. (2020 b, 31474). A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems. IEEE Access. Institute of Electrical and Electronics Engineers (IEEE). http://doi.org/10.1109/access.2020.2973354.

Huang L., Zhang G., Yu S. (2020 c, 31475). A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems. IEEE Access.

Huang L., Zhang G., Yu S. (2020 d, 31479). A Data Storage and Sharing Scheme for Cyber-Physical-Social Systems. IEEE Access. Institute of Electrical and Electronics Engineers (IEEE). http://doi.org/10.1109/access.2020.2973354 .

Jiang Z., Ding Q. (2023, March 15). Second-Order Side-Channel Analysis Based on Orthogonal Transform Nonlinear Regression. Entropy. MDPI AG. http://doi.org/10.3390/e25030505.

Morales Romero J. de J., Reyes Barranca M. A., Tinoco Varela D., Flores Nava L. M., Espinosa Garcia E. R. (2022). SCA-Safe Implementation of Modified SaMAL2R Algorithm in FPGA. Micromachines, 13(11):1872.

Morales Romero J. de J., Reyes Barranca M. A., Tinoco Varela D., Flores Nava L. M., Espinosa Garcia E. R.(2022, October 30).SCA-Safe Implementation of Modified SaMAL2R Algorithm in FPGA. Micromachines. MDPI AG. http://doi.org/10.3390/mi13111872.

Talaki E. B., Savry O., Bouvier Des Noes M., Hely D. (2022 a, April 20). A Memory Hierarchy Protected against Side-Channel Attacks. Cryptography. MDPI AG. http://doi.org/10.3390/cryptography6020019 .

Talaki E. B., Savry O., Bouvier Des Noes M., Hely D. (2022 b , April 20). A Memory Hierarchy Protected against Side-Channel Attacks. Cryptography. MDPI AG. http://doi.org/10.3390/cryptography6020019 .

Talaki E. B., Savry O., Bouvier Des Noes M., Hely D. (2022 c, 6(2):19). A Memory Hierarchy Protected against Side-Channel Attacks. Cryptography.

Zhao Q., Chen S., Liu Z., Baker T., Zhang Y. (2020, November). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Information Processing & Management. Elsevier BV. http://doi.org/10.1016/j.ipm.2020.102355.

Zhao S., Xu S., Han S., Ren S., Wang Y., Chen Z., Liu W. (2024, February 15). PPMM- DA: Privacy-Preserving Multidimensional and Multisubset Data Aggregation With Differential Privacy for Fog-Based Smart Grids. IEEE Internet of Things Journal. Institute of Electrical and Electronics Engineers (IEEE).http://doi.org/10.1109/jiot.2023.3309132. .

CONTENTS

INFORMATICS

Zh.K. Abdugulova, M. Tlegen, A.T. Kishubaeva, N.M. Kisikova, A.K. Shukirova AUTOMATION OF MINING EQUIPMENT USING DIGITAL CONTROL MACHINES.....5

A.A. Abibullayeva, A.S. Baimakhanova
USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES IN KEYWORD EXTRACTION.....25

M. Ashimgaliyev, K. Dyussekeyev, T. Turymbetov, A. Zhumadillayeva
ADVANCING SKIN CANCER DETECTION USING MULTIMODAL DATA FUSION AND AI TECHNIQUES.....37

D.S. Amirkhanova, O.Zh. Mamyrbayev
EL-GAMAL'S CRYPTOGRAPHIC ALGORITHM: MATHEMATICAL FOUNDATIONS, APPLICATIONS AND ANALYSIS.....52

A.Sh. Barakova, O.A. Ussatova, Sh.E. Zhussipbekova, Sh.M. Urazgalieva, K.S. Shadinova
USE OF BLOCKCHAIN FOR DATA PROTECTION AND TECHNOLOGY DRAWBACKS.....67

M. Kantureyev[1], G. Bekmanova, A. Omarbekova, B. Yergesh, V. Franzoni
ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND SOLVING SOCIAL PROBLEMS.....78

A.B. Kassekeyeva, A.B. Togissova*, A.M. Bakiyeva, Z.B. Lamasheva, Y.N. Baibakty ANALYSIS OF COMPARATIVE OPINIONS USING INFORMATION TECHNOLOGY.....88

M. Mussaif, A. Kintonova, A. Nazyrova, G. Muratova, I.F. Povkhan
IMPROVED PUPIL LOCALIZATION METHOD BASED ON HOUGH TRANSFORM USING ELLIPTICAL AND CIRCULAR COMPENSATION.....103

Zh. S. Mutalova, A.G. Shaushenova, G.O. Issakova, A.A. Nurpeisova, M.B. Ongarbayeva, G.A. Abdygalikova
THE METHOD FOR RECOGNIZING A PERSON FROM A FACE IMAGE BASED ON MOVING A POINT ALONG GUIDES.....118

G. Nurzhaubayeva, K. Chezhimbayeva, H. Norshakila
THE DEVELOPMENT AND ANALYSIS OF A WEARABLE TEXTILE YAGI-UDA ANTENNA DESIGN FOR SECURITY AND RESCUE PURPOSES.....138

A.A. Oxenenko, A.S.Yerimbetova, A. Kuanayev, R.I. Mukhamediev, Ya.I. Kuchin
TECHNICAL TOOLS FOR REMOTE MONITORING USING UNMANNED AERIAL PLATFORMS.....152

B.S. Omarov, A.B. Toktarova, B.S. Kaldarova, A.Z. Tursynbayev, R.B. Abdrakhmanov
DETECTING OFFENSIVE LANGUAGE IN LOW-RESOURCE LANGUAGES WITH BILSTM.....174

G.Taganova, D.A. Tussupov, A. Nazyrova, A.A. Abdildaeva, T.Zh. Yermek
SHORT-TERM FORECAST OF POWER GENERATION OF PHOTOVOLTAIC POWER PLANTS BY COMPARING LSTM AND MLP MODELS.....190

Zh. Tashenova, E. Nurlybaeva, Zh.Abdugulova, Sh. Amanzholova
CREATION OF SOFTWARE BASED ON SPECTRAL ANALYSIS FOR STEGOANALYSIS OF DIGITAL AUDIO FILES.....203

Zh.U. Shermantayeva, O.Zh. Mamyrbaev
DEVELOPMENT AND CREATION OF HYBRID EWT-LSTM-RELM- IEWT MODELING IN HIGH-VOLTAGE ELECTRIC NETWORKS.....223

МАЗМҰНЫ

ИНФОРМАТИКА

Ж.К. Абдугулова, М. Тлеген, А.Т. Кишубаева, Н.М. Кисикова, А.К. Шукирова
САНДЫҚ БАСҚАРУ СТАНОКТАРЫНЫҢ КӨМЕГІМЕН ТАУ-КЕН-ШАХТА ЖАБДЫҚТАРЫН АВТОМАТТАНДЫРУ.....5

А.А. Абибуллаева, А.С. Баймаханова
КІЛТТІК СӨЗДЕРДІ ШЫҒАРУДА МАШИНАЛЫҚ ЖӘНЕ ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ.....25

М. Ашимгалиев, К. Дюсекеев, Т. Турымбетов, А. Жумадиллаева
МУЛЬТИМОДАЛЬДЫ ДЕРЕКТЕРДІ БІРІКТІРУ ЖӘНЕ ЖАСАНДЫ ИНТЕЛЛЕКТ ӘДІСТЕРІН ҚОЛДАНА ОТЫРЫП, ТЕРІ ҚАТЕРЛІ ІСІГІН АНЫҚТАУДЫ ЖЕТІЛДІРУ.....37

Д.С. Әмірханова, Ө.Ж. Мамырбаев
ЭЛЬ-ГАМАЛЬДЫҢ КРИПТОГРАФИЯЛЫҚ АЛГОРИТМІ: МАТЕМАТИКАЛЫҚ НЕГІЗДЕРІ, ҚОЛДАНУ ЖӘНЕ ТАЛДАУ.....52

А.Ш. Баракова, О.А.Усатова, Ш.Е.Жусипбекова, Ш.М. Уразгалиева, К.С. Шадинова
ДЕРЕКТЕРДІ ҚОРҒАУДА БЛОКЧЕЙНДІ ПАЙДАЛАНУ ЖӘНЕ ТЕХНОЛОГИЯНЫҢ КЕМШІЛІКТЕРІ.....67

М.А. Кантуреева, Г.Т. Бекманова, А.С. Омарбекова, Б.Ж. Ергеш, V. Franzoni
ЖАСАНДЫ ИНТЕЛЛЕКТТІК ТЕХНОЛОГИЯЛАР ЖӘНЕ ӘЛЕУМЕТТІК МӘСЕЛЕЛЕРДІ ШЕШУ.....78

А.Б. Касекеева, А.Б. Тогисова, А.М. Бакиева, Ж.Б. Ламашева, Е.Н. Байбақты
АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНУ АРҚЫЛЫ САЛЫСТЫРМАЛЫ ПІКІРЛЕРДІ ТАЛДАУ.....88

М. Мұсайф, А.Ж. Кинтонова, А.Е. Назырова, Г. Муратова, И.Ф. Повхан
ЭЛЛИПТИКАЛЫҚ ЖӘНЕ ДӨҢГЕЛЕК КОМПЕНСАЦИЯНЫ ҚОЛДАНА ОТЫРЫП, ХАФ ТҮРЛЕНДІРУІНЕ НЕГІЗДЕЛГЕН КӨЗДІҢ ҚАРАШЫҒЫҢ ЛОКАЛИЗАЦИЯЛАУДЫҢ ЖЕТІЛДІРІЛГЕН ӘДІСІ.....103

Ж.С. Муталова, А.Г. Шаушенова, Г.О. Исакова, А. Нұрпейісова, М.Б. Оңғарбаева, Г.А. Әбдіғалықова
НҮКТЕНІ БАҒЫТТАУШЫЛАР БОЙЫМЕН ЖЫЛЖЫТУ НЕГІЗІНДЕ АДАМДЫ БЕТ БЕЙНЕСІ АРҚЫЛЫ ТАНУ ӘДІСІ.....118

Г. Нуржаубаева, К. Чежимбаева, Х. Норшакила
ҚҰТҚАРУ ҚЫЗМЕТІ МАҚСАТЫНДА КИІМГЕ ОРНАЛАСТЫРЫЛАТЫН ТЕКСТИЛЬДІ ЯГИ-УДА АНТЕННАСЫНЫҢ ДИЗАЙНЫН ҚҰРУ ЖӘНЕ ТАЛДАУ.....138

А.А. Оксененко, А.С. Еримбетова, А. Куанаев, Р.И. Мухамедиев, Я.И. Кучин
ҰШҚЫШСЫЗ ӘУЕ ПЛАТФОРМАЛАРЫН ПАЙДАЛАНАТЫН ҚАШЫҚТАН МОНИТОРИНГ ЖҮРГІЗУ ҮШІН ТЕХНИКАЛЫҚ ҚҰРАЛДАР.....152

Б.С. Омаров, А.Б. Тоқтарова, Б.С. Қалдарова, А.З. Турсынбаев, Р.Б. Абдрахманов
БЕЙӘДЕП СӨЗДЕРДІ АЗ РЕСУРСТЫ ТІЛДЕРДЕН АНЫҚТАУДА BILSTM- ДІ ҚОЛДАНУ.....174

Г.Ж. Таганова, Д.А. Тусупов, А. Назырова, А.А. Абдильдаева, Т.Ж. Ермек
LSTM ЖӘНЕ MLP МОДЕЛЬДЕРІН САЛЫСТЫРУ АРҚЫЛЫ ФОТОЭЛЕКТРЛІК ЭЛЕКТР СТАНЦИЯЛАРЫНЫҢ ЭЛЕКТР ЭНЕРГИЯСЫН ӨНДІРУДІҢ ҚЫСҚА МЕРЗІМДІ БОЛЖАМЫ.....190

Ж.М. Ташенова, Э. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова
САНДЫҚ АУДИОФАЙЛДАРДЫ СТЕГО ТАЛДАУ ҮШІН СПЕКТРАЛДЫ ТАЛДАУ НЕГІЗІНДЕ БАҒДАРЛАМАЛЫҚ ҚҰРАМДЫ ҚҰРУ.....203

Ж.У. Шермантаева, О.Ж. Мамырбаев
ЖОҒАРЫ КЕРНЕУЛІ ЭЛЕКТР ЖЕЛІЛЕРІНДЕ ГИБРИДТІ EWT-LSTM-RELM-IEWT МОДЕЛЬДЕУДІ ДАМЫТУ ЖӘНЕ ҚҰРУ.....223

СОДЕРЖАНИЕ

ИНФОРМАТИКА

Ж.К. Абдугулова, А.Т. Кишубаева, Н.М. Кисикова, А.К. Шукирова
АВТОМАТИЗАЦИЯ ГОРНО-ШАХТНОГО ОБОРУДОВАНИЯ С ПОМОЩЬЮ СТАНКОВ ЦИФРОВОГО УПРАВЛЕНИЯ……5

А.А. Абибуллаева, А.С. Баймаханова
ИСПОЛЬЗОВАНИЕ МЕТОДОВ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ ПРИ ИЗВЛЕЧЕНИИ КЛЮЧЕВЫХ СЛОВ…….....25

М. Ашимгалиев, К. Дюсекеев, Т. Турымбетов, А. Жумадиллаева
СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ВЫЯВЛЕНИЯ РАКА КОЖИ С ИСПОЛЬЗОВАНИЕМ МУЛЬТИМОДАЛЬНОГО ОБЪЕДИНЕНИЯ ДАННЫХ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА……...…37

Д. С. Әмірханова, О. Ж. Мамырбаев
КРИПТОГРАФИЧЕСКИЙ АЛГОРИТМ ЭЛЬ-ГАМАЛЯ:
МАТЕМАТИЧЕСКИЕ ОСНОВЫ, ПРИМЕНЕНИЕ И АНАЛИЗ……....52

А.Ш. Баракова, О.А. Усатова, Ш.Е. Жусипбекова, Ш.М. Уразгалиева, К.С. Шадинова
ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙНА ДЛЯ ЗАЩИТЫ ДАННЫХ И НЕДОСТАТКИ ТЕХНОЛОГИИ…….....67

М.А. Кантуреева, Г.Т. Бекманова, А.С. Омарбекова, Б.Ж. Ергеш, V. Franzon
ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РЕШЕНИЕ СОЦИАЛЬНЫХ ПРОБЛЕМ……...78

А.Б. Касекеева, А.Б. Тогисова, А.М. Бакиева, Ж.Б. Ламашева, Е.Н. Байбақты
АНАЛИЗ СРАВНИТЕЛЬНЫХ МНЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ…….88

М. Мусайф, А.Ж. Кинтонова, А.Е. Назырова, Г. Муратова, И.Ф. Повхан
УЛУЧШЕННЫЙ МЕТОД ЛОКАЛИЗАЦИИ ЗРАЧКА НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ХАФА С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКОЙ И КРУГОВОЙ КОМПЕНСАЦИИ……..…..103

Ж.С. Муталова, А.Г. Шаушенова, Г.О. Исакова, А.А. Нурпейсова, М.Б. Онгарбаева, Г.А. Абдыгаликова
МЕТОД РАСПОЗНАВАНИЯ ЧЕЛОВЕКА ПО ИЗОБРАЖЕНИЮ ЛИЦА НА ОСНОВЕ ПЕРЕМЕЩЕНИЯ ТОЧКИ ПО НАПРАВЛЯЮЩИМ……118

Г. Нуржаубаева, К. Чежимбаева, Х. Норшакила
РАЗРАБОТКА И АНАЛИЗ ДИЗАЙНА ВСТРАИВАЕМОЙ ТЕКСТИЛЬНОЙ ЯГИ-УДА АНТЕННЫ ДЛЯ ПРИМЕНЕНИЯ В СФЕРЕ СПАСАТЕЛЬНЫХ СЛУЖБ.....138

А.А. Оксененко, А.С. Еримбетова, А. Куанаев, Р.И. Мухамедиев, Я.И. Кучин
ТЕХНИЧЕСКИЕ СРЕДСТВА ДИСТАНЦИОННОГО МОНИТОРИНГА С ПОМОЩЬЮ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ ПЛАТФОРМ…….152

Б.С. Омаров, А.Б. Токтарова, Б.С. Калдарова, А.З. Турсынбаев, Р.Б. Абдрахманов
ИСПОЛЬЗОВАНИЕ BILSTM ДЛЯ ОПРЕДЕЛЕНИЯ ОСКОРБИТЕЛЬНОГО ЯЗЫКА В ЯЗЫКАХ С НИЗКИМ УРОВНЕМ РЕСУРСОВ…….....….174

Г.Ж. Таганова, Д.А. Тусупов, А. Назырова, А.А. Абдильдаева, Т.Ж. Ермек
КРАТКОСРОЧНЫЙ ПРОГНОЗ ВЫРАБОТКИ ЭЛЕКТРОЭНЕРГИИ ФОТОЭЛЕКТРИЧЕСКИМИ ЭЛЕКТРОСТАНЦИЯМИ ПУТЕМ СРАВНЕНИЯ МОДЕЛЕЙ LSTM И MLP.....190

Ж.М. Ташенова, Э. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова
СОЗДАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА БАЗЕ СПЕКТРАЛЬНОГО АНАЛИЗА ДЛЯ СТЕГОАНАЛИЗА ЦИФРОВЫХ АУДИОФАЙЛОВ.....203

Ж.У. Шермантаева, О.Ж. Мамырбаев
РАЗРАБОТКА И СОЗДАНИЕ ГИБРИДНОГО МОДЕЛИРОВАНИЯ EWT-LSTM-RELM-IEWT В ВЫСОКОВОЛЬТНЫХ ЭЛЕКТРИЧЕСКИХ СЕТЯХ.....223

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 30.09.2024.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
15,5 п.л. Тираж 300. Заказ 3.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19