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

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (346)

APRIL – JUNE 2023

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/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«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/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

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/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Namber 346 (2023). 5–20
https://doi.org/10.32014/2023.2518-1726.180

UDK 004-056-5

© A. Adamova[1*], T. Zhukabayeva[2], Y. Mardenov[3], 2023
[1] Astana IT University, Astana, Kazakhstan;
[2] L. Gumilyov Eurasian National University, Astana IT University, Astana, Kazakhstan;
[3] Astana International University, Astana, Kazakhstan.
E-mail: aigul.adamova@astanait.edu.kz

INTERNET OF THINGS: STATUS AND PROSPECTS FOR THE DEVELOPMENT OF LIGHTWEIGHT ALGORITHMS

Adamova Aigul — Doctor PhD of Computing and Software Engineering, Assistant Professor, Department of Computer Engineering, Astana IT University, Astana, Kazakhstan
E-mail: aigul.adamova@astanait.edu.kz. ORCID ID: 0000-0001-7773-9522;
Zhukabayeva Tamara — PhD (Informatics, Computer Engineering and Control), Associate Professor), Department of Information Systems, L. Gumilyov Eurasian National University, Astana IT University, Astana, Kazakhstan
E-mail: tamara.kokenovna@gmail.com. ORCID ID: 0000-0001-6345-5211;
Mardenov Yerik — PhD. Doctoral student. Astana International University, Astana, Kazakhstan
E-mail: emardenov@gmail.com. ORCID ID: 0000-0001-9284-9797.

Abstract. There is a high probability of various attacks coming from unknown network devices, in this regard, ensuring the security and confidentiality of data is relevant and one of the main problems today. It is important to note that IoT has a number of limitations in terms of power supply, memory and dimensions. Thus, it is necessary to define more resource-optimized and security-related inferences to solve the problems generated in the network. Along with this, device resources are consumed at a higher rate due to complex cryptographic maintenance algorithms, so it is necessary to determine an appropriate encryption procedure for an automated IoT network, taking into account data integrity. This article presents an analysis of lightweight algorithms for hardware and software implementation, the levels of various data flow architectures in the IoT network are considered, an overview of scientific papers is given that notes the relevance of ensuring security in the interaction of IoT devices and the development of lightweight cryptography for 2022–2023. As a result, the results of a comparative analysis of lightweight algorithms in terms of several indicators for hardware implementation are given; when implemented in software, relative to the amount of memory and time delay.

Keywords: Internet of Things, security, privacy, lightweight encryption, lightweight cryptography

Financing: This research has been/was/is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP14973006).

Conflict of interest: The authors declare that there is no conflict of interest.

© А. Адамова[1*], Т. Жукабаева[2], Е. Марденов[3], 2023

[1] Astana IT University, Астана, Казахстан;
[2] Евразийский национальный университет им. Л. Гумилева, Астана, Казахстан;
[3] Международный университет Астана, Астана, Казахстан.
E-mail: aigul.adamova@astanait.edu.kz

ЗАТТАР ИНТЕРНЕТІ: ЖЕҢІЛДІК АЛГОРИТМДЕРДІҢ ДАМУЫ ЖӘНЕ БОЛАШАҒЫ

Адамова Айгуль — Есептеу техникасы және бағдарламалық қамтамасыз ету мамандығы бойынша философия докторы (PhD), Компьютерлік инженерия департаментінің профессор ассистенті. Astana IT University. Астана, Қазақстан
E-mail: aigul.adamova@astanait.edu.kz. ORCID ID: 0000-0001-7773-9522;
Zhukabayeva Tamara — Информатика, есептеу техникасы және бақылау мамандығы бойынша философия докторы (PhD), Ақпараттық жүйелер кафедрасының профессор м.а., қауымдастырылған профессор. Л.Н.Гумилев атындағы Еуразия ұлттық университеті. Астана, Қазақстан
E-mail: tamara.kokenovna@gmail.com. ORCID ID: 0000-0001-6345-5211;
Mardenov Yerik — PhD Докторанты. Астана халықаралық уни верситеті. Астана, Қазақстан
E-mail: emardenov@gmail.com. ORCID ID: 0000-0001-9284-9797.

Аннотация. Белгісіз желілік құрылғылардан келетін әртүрлі шабуылдардың үлкен ықтималдығы бар, осыған байланысты деректердің қауіпсіздігі мен құпиялылығын қамтамасыз ету өзекті және бүгінгі күні негізгі мәселелердің бірі болып табылады. IoT-те қуат, жады және бірқатар өлшемдер бойынша шектеулер бар екенін ескеру маңызды. Осылайша, желіде туындаған мәселелерді шешу үшін ресурстардың оңтайландырылған және қауіпсіздікке қатысты қорытындыларды анықтау қажет. Сонымен қатар, күрделі криптографиялық қызмет алгоритмдеріне байланысты құрылғы ресурстары жоғары жылдамдықпен қолданады, сондықтан деректердің тұтастығын ескере отырып, автоматтандырылған IoT желісі үшін қолайлы шифрлау процедурасын анықтау қажет. Бұл мақалада аппараттық және бағдарламалық қамтамасыз етуді іске асырудағы жеңіл салмақ алгоритмдерін талдау, IoT желісіндегі әртүрлі деректер ағынының архитектураларының деңгейлері қарастырылған, IoT құрылғыларының өзара әрекеттесуіндегі қауіпсіздікті қамтамасыз етудің өзектілігін және 2022–2023 жылдардағы жеңіл салмақ криптографиясының дамуын атап өтетін ғылыми жұмыстарға

шолу берілген. Нәтижелер ретінде аппараттық іске асыру кезінде бірнеше көрсеткіштер бойынша жеңіл салмақтағы алгоритмдерді салыстырмалы талдау нәтижелері келтірілген; онымен қоса жады көлеміне және уақыт кідірісіне қатысты бағдарламалық іске асыру қорытындылары көрсетілген.

Түйін сөздер: Интернет заттар, қауіпсіздік, құпиялылық, жеңіл шифрлау, жеңіл криптография

Қаржыландыру: Бұл зерттеу Қазақстан Республикасы Ғылым және жоғары білім министрлігі, Ғылым комитетімен қаржыландырған (Грант № BR10262555).

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдемейді.

© А. Адамова[1*], Т. Жукабаева[2], Е. Марденов[3], 2023

[1] Astana IT University, Астана, Казахстан;
[2] Евразийский национальный университет им. Л. Гумилева, Астана, Казахстан;
[3] Международный университет Астана, Астана, Казахстан.
E-mail: aigul.adamova@astanait.edu.kz

ИНТЕРНЕТ ВЕЩЕЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЛЕГКОВЕСНЫХ АЛГОРИТМОВ

Адамова Айгуль — доктор PhD. Ассистент профессора. Департамент компьютерной инженерии. Astana IT University. Астана, Казахстан
E-mail: aigul.adamova@astanait.edu.kz. ORCID ID: 0000-0001-7773-9522;
Zhukabayeva Tamara — доктор PhD. и.о. профессора, ассоциированный профессор. Кафедра информационных систем. Евразийский национальный университет им.Л.Н.Гумилева. Астана, Казахстан
E-mail: tamara.kokenovna@gmail.com. ORCID ID: 0000-0001-6345-5211;
Mardenov Yerik — Докторант PhD. Международный университет Астана. Астана, Казахстан
E-mail: emardenov@gmail.com. ORCID ID: 0000-0001-9284-9797.

Аннотация. Существует большая вероятность различных атак, исходящих от неизвестных устройств сети, в связи с этим обеспечение безопасности и конфиденциальности данных являются актуальным и одним из основных проблем на сегодняшний день. Важно отметить, что IoT имеет ряд ограничений по запасу электропитания, памяти и габаритов. Таким образом, необходимо определить более оптимизированные для ресурсов и связанные с безопасностью выводы для решения проблем, генерируемых в сети. Вместе с этим, ресурсы устройств потребляются с более высокой скоростью из-за сложных криптографических алгоритмов обслуживания, поэтому необходимо определить подходящую процедуру шифрования для автоматизированной сети IoT с учетом целостности данных. В данной статье представлен анализ легковесных алгоритмов при аппаратной и программной

реализации, рассмотрены уровни различных архитектур потока данных в сети IoT, приведены обзор научных работ отмечающих актуальность обеспечения безопасности при взаимодействии IoT устройств и развитие легковесной криптографии за 2022–2023 года. В качестве результатов приведены результаты сравнительного анализа легковесных алгоритмов по нескольким показателям при аппаратной реализации; при программной реализации относительно объема памяти и задержки по времени.

Ключевые слова: Интернет вещей, безопасность, конфиденциальность, легковесное шифрование, легковесная криптография

Финансирование: Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (Грант № BR10262555).

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction

The Internet of Things (IoT) is an intelligent infrastructure formed using several self-organizing devices. Currently, the "IoT" can be defined as an intelligent infrastructure of interacting physical objects in the form of sensors and actuators with the digital world (Vermesan et al., 2009: 52), which transmits information using a network. There are many applications where systems are deployed using IoT. In everyday life, people use many devices, which include sensors to detect problems, transmit information, monitor, control, and so on. The information is provided in real time and can be used to make a decision; therefore, the security and confidentiality of information is a very important aspect. It is also important that the IoT has a number of limitations in terms of power supply, memory and dimensions. Along with this, it is important to determine suitable encryption methods for the IoT network in order to ensure data integrity (Eryk et al., 2022: 18).

According to Statista, the number of attacks on the Internet of Things in 2022 exceeded 10.54 million. Ensuring security in IoT interaction is one of the important tasks of the present time. One of the current methods for ensuring the security and confidentiality of transmitted data in a network of IoT devices is lightweight cryptography algorithms. The National Institute of Standards and Technology NIST conducts research in this area and scientists around the world in search of optimally suitable lightweight algorithms used in IoT devices. So scientists from Graz Technology University (Austria), chip manufacturing company Infineon Technologies (Germany), Lamarr Security Research (Austria) and Radboud University (Netherlands) are working on security and privacy issues,

Encryption is an effective solution to ensure the confidentiality of information and its integrity. Today, IoT applies encryption to touch devices in environments with various restrictions, such as limited memory, low computing power, small physical area, devices with limited power consumption, and at the same time, processes must

take place in real time,that have not previously been encrypted. When designing IoTthere are a number of risks directly related to energy consumption and data security. If standard cryptography methods are applied to IoT devices, they may not support the given performance and not only, respectively, for these problems, the solution can be - lightweight cryptography (Nurlan et al., 2021: 19).

This article consists of two sections, which discusses the IoT architecture, development stages, parameters, lightweight cryptography standards, an overview of the work, and also provides an analysis of the numerical characterstics of the hardware and software implementation of lightweight algorithms.

IoT architecture

There are several types of IoT architecture, such as three-, four-, five-layer architectures (Figure 1). Table 1 shows scientists - whose research is carried out on various architectures. To determine the relevance and degree of resolution of the issue under consideration, a search and review of scientific papers in the databases of digital libraries "Web Of Science", "Google Scholar", "IEEE Xplore" was carried out.The review paper (Muhammad et al., 2022: 12) discusses the importance of IoT network security, considers various threats depending on the IoT architectural model. The paper also presents lightweight cryptographic algorithms and protocols for data protection in the IoT environment. S.L. Keoh et al presented an overview of the IEFT (Internet Engineering Task Force) requirements for standardizing security solutions in the IoT network (Keoh, et al., 2014: 10). P. Gaikweid et al presented the IoT architecture associated with the attack model. As mentioned above, IoT is used in various applications, for example, a smart home network can control home devices and appliances, controlling and remotely controlling through various connection methods. The paper also presents some problems in the mode and real time (Gaikwad et al., 2015: 6). It is important to note that depending on the IoT architecture and the level under consideration, various security solutions can be selected for the interaction of IoT devices.

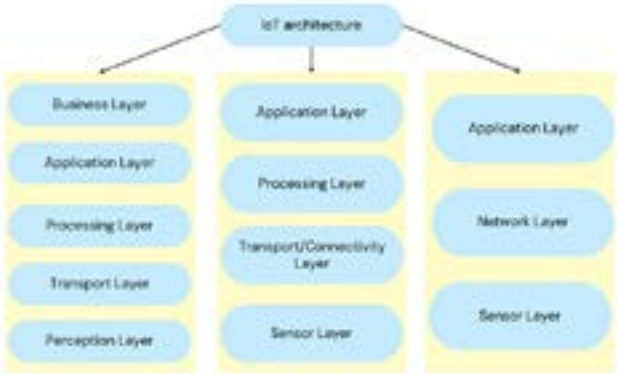

Fig. 1. Layers of different IoT data flow architectures

Consider a three-layer architecture:

- The level of sensors is the physical level, which consists of sensors and sensors responsible for collecting information about the surrounding world. At the sensor level, the IEEE 802.15.4 standard is used as a specification. It's an affordable solution that provides security, but still needs to address existing threat protection loopholes. For example, RFID, various sensors for location, motion, voice, etc. Possible attacks at the sensor level — jamming, tampering, radio interference, unfairness, exhaustion, collisions (Singh et al., 2020: 12);

- Network layer - serves to communicate with other network objects, such as servers, network devices, etc. Here we can note the method of interaction with each other — a wireless sensor network or Internet protocols. The network layer works with the physical layer data. It is also used to disseminate and analyze sensor data. At the network level, the message is divided into packets in order to route packages from source to destination using IPv6. With IoT networks growing rapidly, IPv4 address space has an advantage over IPv6 with more address spaces. Built-in cryptographic conventions such as AES and DES can be updated with IPsec at this level. Attacks possible at the network level — Sinkhole, blackhole, wormhole, misdirection, homing (Singh et al., 2020: 12);

- Application level — the level of applications that provide a special service for working with data and managing them. The application layer is responsible for providing the user with resources regarding the application being used. This layer supports services for client and programmatic functions. As an example, various classes of IoT solutions can be noted: Smart city, smarthome, digital factories, precision farming oil, etc. Attacks possible at the application level — Reprogram, Overwhelm (Singh et al., 2020: 12).

Table - 1. IoT architecture

Type of Architecture	Year	Authors	Name of the Journal
Three-layer architecture	2015	I. Mashal et al.	Ad Hoc Networks Journal
	2022	Aguru, A.D. et al.	Algorithms
	2022	B. Paul	Lecture Notes in Networks and Systems
	2020	M. Parto	Procedia Manufacturing
	2016	F. Bing	2016 2nd International Conference on Cloud Computing and IoT
	2022	B. Paul	ICT Analysis and Applications
Four-layer architecture	2017	C. Zhong et al.	16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science
	2013	J. Gubbi et al.	Future Generation Computer Systems Journal
	2022	Denner Silva et al.	Journal of Network & Systems Management
	2019	J. Li et al.	IEEE Access
	2017	S. Singh et al.	Journal of Ambient Intelligence and Humanized Computing
	2018	C. Kejun	Journal of Hardware and Systems Security
	2015	D. Darwish	International Journal of Computing Academic Research

Five-layer architecture	2022	Raja Gopal, S. et al.	International Journal of System Assurance Engineering and Management
	2017	P. Sethi et al.	Journal of Electrical and Computer Engineering
	2022	Jinyuan Xu et al.	Artificial Intelligence in Agriculture
	2013	S. Omar et al.	International Journal of Computer Networks
	2022	A. Khaled et al.	Journal of Cloud Computing
	2021	M. Yıldırım et al.	European Journal of Science and Technology

IoT device security concerns arise in a variety of situations that include technological, ethical, and privacy issues. IoT devices will be considered secure if the following security requirements are met, such as secure authentication, secure download and data transfer, IoT data security, secure access to data by an authorized person. Figure 2 shows the threats and security requirements of a three-layer architecture. The sensor layer is the perception layer and is responsible for identifying devices and collecting information from them. The sensors are selected according to the requirements of the applications. Information that is collected at the level of sensors can be information about location, changes in the air, about the environment, about movement, about vibration, etc. At the same time, this information is the main goal of attackers who want to use them to achieve their own goals. Therefore, most threats are related to the level of sensors and lightweight encryption methods have a special role.

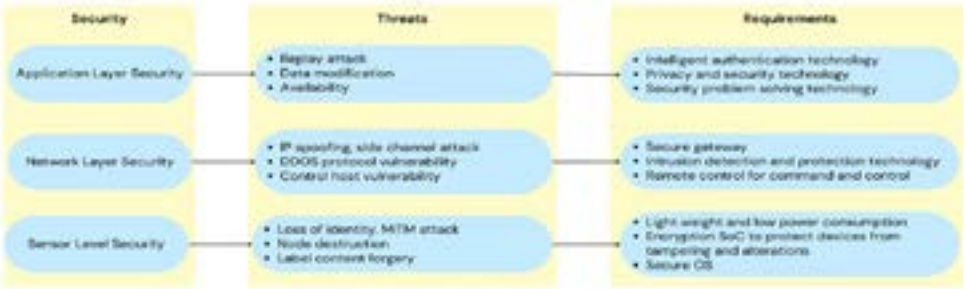

Fig. 2. Threats and security requirements based on a three-layer architecture

Lightweight cryptography in IoT

Lightweight cryptography is divided into two ciphers: a symmetric cipher and an asymmetric cipher. If a symmetric cipher uses the same key for both encryption and decryption, an asymmetric cipher uses the public key for encryption and the private key for decryption. Symmetric encryption provides security and high speed, along with this, an asymmetric cipher is complex and relatively slow, but at the same time, it ensures the confidentiality and integrity of data. The symmetric cipher is divided into three groups: the lightweight block cipher, the lightweight hash function, and the lightweight stream cipher. The classification of lightweight cryptography, the most common algorithms and attacks is shown in Figure 3.

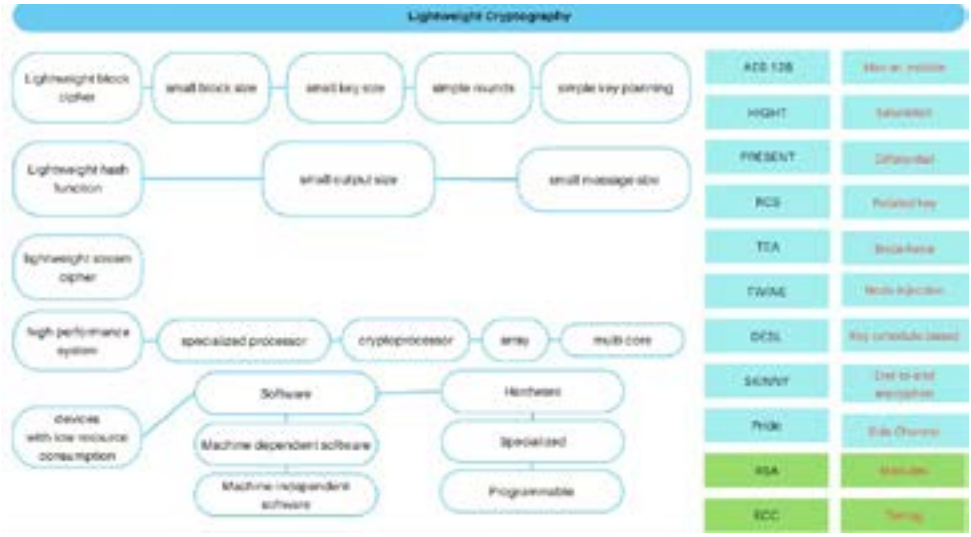

Fig. 3. Classification of algorithms by structure

Research in the direction of lightweight cryptography was started in 2004. In 2007, the PRESENT block cipher was developed and published, which was registered in the ISO / IEC 29192 standard. The US National Security Agency published the SIMON / SPECK lightweight block cipher with a small ROM size and implemented it on a microprocessor (2014). The main stages in the development of lightweight cryptography are shown in Figure 4.

Fig. 4. Stages of development of lightweight cryptography

Lightweight Cryptography Options

One of the important properties of lightweight algorithms is the non-linearity of the coordinate functions of the round transformation (Poschmann, 2009: 516). The nonlinearity of the coordinate function of the output block is determined using the minimum number of rounds.

There are randomly selected options. For these parameters $x, x', p \in S_n, p \neq 0$

, vectors are encrypted $x, x', x+p, x'+p$. The transformation is non-linear if the condition is satisfied $f(x)+f(x+p) \neq f(x')+f(x'+p)$.

The superposition of non-linear functions produces a system of linear equations:

$$f_1(x,y) = x \oplus y \oplus xy$$
$$f_2(x,y) = x \oplus xy$$

When setting functions instead of , the following system of equations is obtained:

$$f_1(f_1(x,y), f_2(x,y)) = x \oplus y \oplus xy$$

When learning lightweight cryptography, you need to consider the main criteria for security, cost and performance. In the case of block ciphers, the key length provides a trade-off between security and cost, the number of rounds is a trade-off between security and performance, and the hardware is a trade-off between cost and performance (Figure 5). Considering all three trade-offs at the same time is challenging, and two design goals are mainly considered — safety and low cost, safety and productivity, or low cost and productivity. For example, a secure and high performance hardware implementation can be achieved with a pipelined architecture that also includes many side-channel attack countermeasures. The resulting structure will occupy a large area, which is correlated with high costs. On the other hand, it is possible to develop a secure and inexpensive hardware implementation with the disadvantage of limited performance.

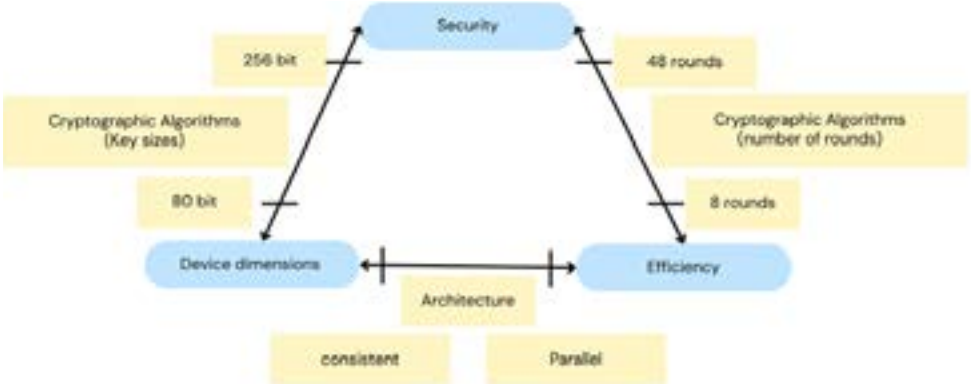

Fig. 5. Lightweight Cryptography Options

Table 2 summarizes the main challenges of implementing cryptographic algorithms in IoT devices and lightweight cryptography solutions.

Table 2. Lightweight Cryptography Options

Implementation challenges in IoT devices	Lightweight Cryptography Solutions
limited memory (registers, RAM, ROM)	small block size (64-bit or less)
low processing power	small key size (80-bit or less)
small physical area	simple logic and simple calculations
low battery (no battery)	simple key planning
work in real time	reliable structure (SPN or FN) [5]

Shannon in his work proposed to use several stages of replacement and permutation, thereby creating a reliable block cipher (Shannon E., et al, 1949:59). Such a scheme is called an SP or FN network. SP- processes the data through a series of substitutions (S-box) and permutations (table), changing the data and finalizing it for the next round. FN is a multi-round cipher that divides the input message into two parts and operates on only one part in each round of encryption or decryption.

ISO/IEC 29192 "Lightweight Cryptography" is an eight-part standard that defines lightweight cryptographic algorithms for privacy, authentication, identification, security, and key exchange (Table-3) (https://webstore.iec.ch).

Table - 3. Lightweight Cryptography Standards

Standard	Description	Summary
ISO/IEC 29192-1:2012	General Information	Terms and Definitions; Safety requirements, Classification requirements; Implementation requirements for mechanisms
ISO/IEC 29192-2:2019	Block Encryption	Three block ciphers are described that are suitable for applications requiring lightweight cryptographic implementations: - PRESENT: simplified block cipher / block size 64 bits / key size 80/128 bits; - CLEFIA: lightweight block cipher / block size 128 bits / key size 128/192/256 bits; - LEA: Lightweight block cipher/block size 128 bits/key size 128/192/256 bits
ISO/IEC 29192-3:2012	Stream Ciphers	Defines keystream generators for lightweight stream ciphers: - Enocoro: lightweight keystream generator with 80/128 bit key size; - Trivium: lightweight keystream generator with 80 bit key size
ISO/IEC 29192-4:2013	Mechanisms using asymmetric methods	Defines lightweight mechanisms that use asymmetric methods: - one-way authentication mechanism based on discrete logarithms on elliptic curves; - Authenticated Lightweight Key Exchange (ALIKE) mechanism for one-way authentication and session key establishment; - identification-based signature mechanism
ISO/IEC 29192-4:2013/ AMD1:2016	Mechanisms using asymmetric methods	Updated version

ISO/IEC 29192-5:2016	hash function	Defines hash functions suitable for applications requiring lightweight cryptographic implementations. - PHOTON: lightweight hash function/permutation size 100/144/196/256/288 bits/calculated hash codes 80/128/160/224/256 bits. - SPONGENT: lightweight hash function/permutation size 88/136/176/240/272 bits/calculated hash codes 88/128/160/224/256 bits. - Lesamnta-LW: lightweight hash function/permutation size 384 bits/computed hash code 256 bits
ISO/IEC 29192-6:2019	Message Authentication Code (MACs)	MAC algorithms suitable for applications requiring lightweight cryptographic mechanisms have been defined: - a mechanism for ensuring data integrity; - message authentication mechanism
ISO/IEC 29192-7:2019	Broadcast Authentication Protocols	Defines broadcast authentication protocols, which are protocols that provide data integrity and entity authentication in a broadcast setting
ISO/IEC 29192-8:2022	Authenticated Encryption	An authenticated encryption method suitable for applications requiring lightweight cryptographic mechanisms is described. The method processes the data string with the following security objectives: - data confidentiality; - data integrity

In the table-4 presents scientific papers published in 2022–2023 devoted to the problems of cryptography and security in the context of the Internet of things (IoT). The table lists the titles of articles, authors, year of publication, and a brief abstract for each article.

Table - 4. Review of works on lightweight IoT encryption for 2022–2023.

Authors	Year	Annotation
P. Prakasam et al.	2022	The paper proposes and implements a hybrid lightweight cryptographic authentication scheme with low latency, area and optimal power, which uses the 8-bit keying principle.
S. Blank et al.	2022	The paper presents the practical results of research of 12 cryptographic algorithms on a test bench
A. Kumar et al.	2022	The paper presents a literature review of post-quantum cryptography for IoT networks, discusses the problems and directions of research in real-time applications.
K. Tsantikidou et al.	2022	The paper investigates well-known lightweight cryptographic algorithms and their architecture. The analysis of security algorithms, architecture and hardware limitations in healthcare applications is given.
S. Alshehri et al.	2022	The paper proposes an attribute-based access control scheme for IoT using the Hyperledger Fabric blockchain to solve security problems. Performance metrics are measured based on latency, throughput, and storage overhead,
T. Goyal et al.	2022	The paper presents the results of hardware implementation of PRESENT, AES, ECDH, DH and RSA cryptography algorithms.

Sheeja S. et al.	2022	The paper presents approaches to authentication in the IoT-Cloud architecture.
M. Jammula et al.	2022	The paper presents the LWC-ABE method for improving security performance against various attacks in the IoT environment.
A. Ahmed et al.	2023	The paper investigates integration systems between authentication and encryption to preserve confidentiality when passing messages between IoT devices.
J. Chauhan et al.	2023	This paper presents a comparison of their memory performance, latency and throughput, area (GE), key and block size, and other parameters of hardware and software efficient lightweight algorithms.

Lightweight algorithms are designed to protect the transmitted information during the interaction of the Internet of things, at the same time, lightweight algorithms are used in miniature devices where a limited amount of electronic resources is used to ensure security. Today, many researchers from different countries continue to search for weaknesses and identify reliable and efficient algorithms for lightweight cryptography. The choice of the optimal cryptographic algorithm depends on the specific requirements and constraints of the system, including hardware resources, power, power consumption, and performance requirements.

The hardware implementation of lightweight algorithms is determined by the following parameters (Figure 6):

- key size;
- block size;
- logical process;
- Energy consumption;
- throughput;
- hardware performance.

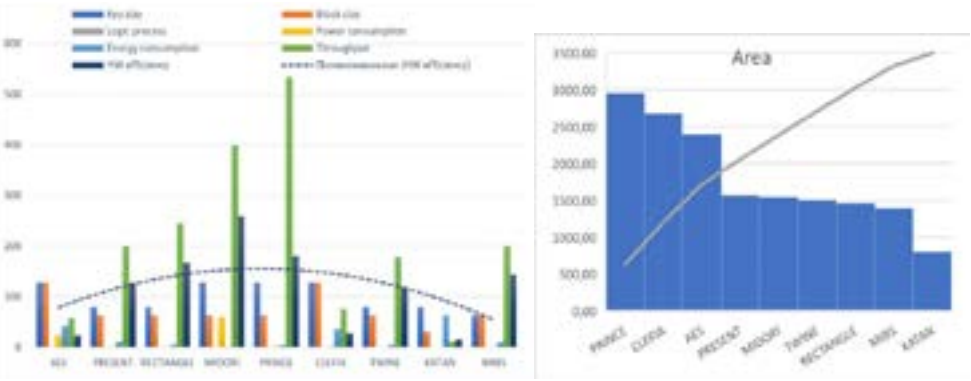

Fig. 6. Numerical characteristics of the hardware implementation of lightweight algorithms

The diagram shows the number of gates in hardware implementation and you can see that the high throughput is achieved by the “PRINCE” algorithm with a

minimum power consumption indicator (Figure 6). Various FPGA families are used as a platform for implementing lightweight algorithms.

The software implementation of lightweight algorithms is described using parameters (Figure 7):

- key size;
- block size;
- RAM size;
- Energy consumption;
- throughput;
- software performance;

Additionally, diagrams are given with the dimensions of the read-only memory and the time delay.

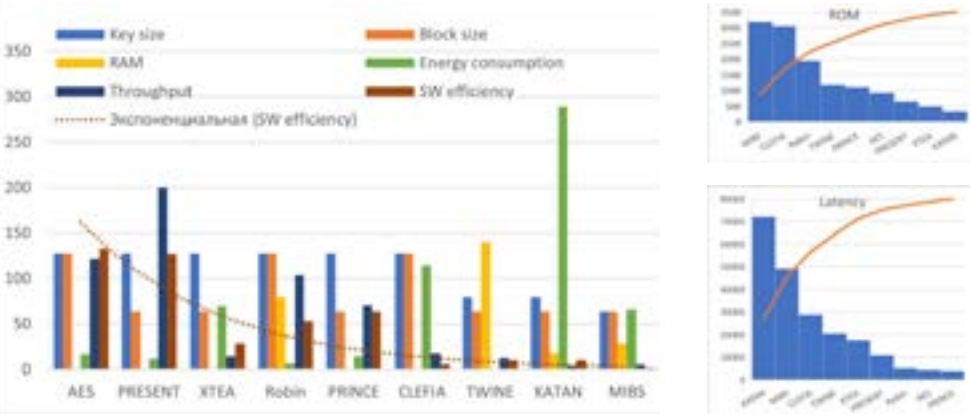

Fig.7. Numerical characteristics of software implementation of lightweight algorithms

The diagram shows several lightweight algorithms such as SPN and FN. According to the diagram, in software implementation, the “PRESENT” algorithm dominates in terms of bandwidth, the “MIBS” algorithm in terms of power consumption and memory space occupied in ROM, and the lowest time delay is demonstrated by the “PRINCE” algorithm (Figure 7).

Conclusion

The Internet of Things (IoT) is rapidly finding its way into our modern lives, seeking to improve the quality of life by connecting various smart devices, technologies and applications. In general, if you choose the right lightweight security algorithm, then IoT will automate everything that surrounds us. The wide range of IoT applications in various fields creates a demand for lightweight cryptographic algorithms with different requirements. Smart home appliances such as smart TV, smart refrigerator, smart kettle, smart light bulbs, etc. require little memory and little processing power. Lightweight algorithms must support simple hardware and software implementation for fast execution, so that it can be

easily embedded in software for encryption, protection transmission and storage data in real applications. When using IoT, an organization faces the challenge of managing, monitoring and securing huge amounts of data and connections from disparate devices.

The paper presents the architecture of IoT devices, an overview of lightweight cryptographic algorithms, threats and security requirements based on a three-layer architecture, lightweight cryptography primitives regarding key size, block length, number of rounds and structure, as well as classification and parameters of lightweight cryptography. Descriptions of sections of ISO/IEC 29192 "Lightweight cryptography" were presented. The works of the authors, who in their studies considered various types of architectures in relation to the tasks to be solved, are summarized. The security problems of IoT devices are considered, as well as a review of works on lightweight IoT encryption for 2022-2023.

This article provides an overview of various studies about layered IoT architectures. Along with the exponential growth in the number of connected devices, every thing in the IoT transmits data packets that require reliable connectivity, storage, and security. The hardware and software implementation of lightweight algorithms is analyzed in terms of such parameters as key size, block size, logical process, power consumption, bandwidth, hardware performance, RAM size, software. Taking into account the growth of attacks and threats on the IoT infrastructure, the discussed issues of lightweight cryptography need to be further studied and developed to ensure sufficient security.

REFERENCES

Aguru A., Babu E., Nayak S., Sethy A., Verma A., 2022 — *Aguru A., Babu E., Nayak S., Sethy A., Verma A.* Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation. Algorithms, 15: 309. https://doi.org/10.3390/a15090309. (in Eng.).

Ahmed A.A., Malebary S.J., Ali W., Alzahrani A.A., 2023 — *Ahmed A.A., Malebary S.J., Ali W., Alzahrani A.A.* A Provable Secure Cybersecurity Mechanism Based on Combination of Lightweight Cryptography and Authentication for Internet of Things. Mathematics, 11(1):220. (in Eng.).

Alaghbari K., Md S., Mohamad H., Hussain A., Alam M., 2022 — *Alaghbari K., Md S., Mohamad H., Hussain A., Alam M.* Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations. Journal of Cloud Computing. 11:65. (in Eng.).

Alshehri S., Bamasag O., 2022 — *Alshehri S., Bamasag O.* AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain. Applied Sciences, 12(16):8111. (in Eng.).

Blanc S., Lahmadi A., Gouguec K., Minier M., Sleem L., 2022 — *Blanc S., Lahmadi A., Gouguec K., Minier M., Sleem L.* Benchmarking of lightweight cryptographic algorithms for wireless IoT networks. Wireless Networks. 28(8). Pp. 3453–3476. (in Eng.).

Bonani P., 2022 — *Bonani P*. Internet of Things (IoT), Three-Layer Architecture, Security Issues and Counter Measures. ICT Analysis and Applications. Springer Nature Singapore, 2022. (in Eng.).

Chauhan J.A., Patel R.A., Parikh S., Modi N., 2022 — *Chauhan J.A.*, *Patel R.A., Parikh S., Modi N.* An Analysis of Lightweight Cryptographic Algorithms for IoT-Applications. Advancements in Smart Computing and Information Security. Springer Nature Switzerland, 2023. Pp. 201–216. (in Eng.).

Chen K., Zhang S., Li Z., Zhang Y., Deng Q., Ray S., Jin Y., 2018 — Chen K., Zhang S., Li Z., Zhang Y., Deng Q., Ray S., Jin Y. Internet-of-Things Security and Vulnerabilities: Taxonomy,

Challenges, and Practice. Journal of Hardware and Systems Security, 2(2). Pp. 97–110. (in Eng.).

Darwish D., 2015 — *Darwish D.*, "Improved layered architecture for Internet of Things," Int. J. Comput. Acad. Res.(IJCAR), 4. Pp. 214–223. (in Eng.).

Eryk C., Andy A., Jara F., Jonathan S., Michael Z., Burkhard S., 2022 — *Eryk C., Andy A., Jara F., Jonathan S., Michael Z., Burkhard S.* Landscape of IoT security, Computer Science Review, 44: 100467. ISSN 1574–0137. https://doi.org/10.1016/j.cosrev.2022.100467. (in Eng.).

Fu Bing, 2016 — *Fu Bing.* The research of IOT of agriculture based on three layers architecture. 2016 2nd International Conference on Cloud Computing and Internet of Things (CCIOT), 2016. Pp. 162–165. doi: 10.1109/CCIOT.2016.7868325.

Gaikwad P.P., Gabhane J.P., Golait S.S., 2015 — *Gaikwad P.P., Gabhane J.P., Golait S.S.* 3-level secure Kerberos authentication for Smart Home Systems using IoT. 2015 1st International Conference on Next Generation Computing Technologies (NGCT), 2015. Pp. 262–268, doi: 10.1109/NGCT.2015.7375123. (in Eng.).

Goyal T.K., Sahula V., Kumawat D., 2022 — *Goyal T.K., Sahula V., Kumawat D.* Energy efficient lightweight cryptography algorithms for IoT devices. IETE Journal of Research, 68(3). Pp. 1722–1735. (in Eng.).

Gubbi J., Buyya R., Marusic S., Palaniswami M., 2013 — *Gubbi J., Buyya R., Marusic S., Palaniswami M.* Internet of Things (IoT): a vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7). Pp.1645–1660. (in Eng.).

IEC, 2023 - *IEC* https://webstore.iec.ch/ (in Eng.).

Jammula M., Vakamulla V.M., Kondoju S.K., 2022 — *Jammula M., Vakamulla V.M., Kondoju S.K.* Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system. Connection Science, 34(1). Pp. 2431–2447. (in Eng.).

Jinyuan Xu, Baoxing Gu, Guangzhao Tian, 2022 — *Jinyuan Xu, Baoxing Gu, Guangzhao Tian.* Review of agricultural IoT technology. Artificial Intelligence in Agriculture, 6. Pp.10–22. ISSN 2589–7217. https://doi.org/10.1016/j.aiia.2022.01.001. (in Eng.).

Keoh S.L., Kumar S.S., Tschofenig H., 2014 — *Keoh S.L., Kumar S.S., Tschofenig H.* Securing the Internet of Things: A Standardization Perspective. IEEE Internet of Things Journal, 1(3). Pp. 265–275. doi: 10.1109/JIOT.2014.2323395. (in Eng.).

Kumar A. et al., 2022 — *Kumar A. et al.* Securing the future internet of things with postquantum cryptography. Security and Privacy, 5(2): e200. (in Eng.).

Li J. et al., 2019 — *Li J. et al.* A Remote Monitoring and Diagnosis Method Based on Four-Layer IoT Frame Perception. IEEE Access, 7:144324–144338. doi: 10.1109/ACCESS.2019.2945076. (in Eng.).

Mahmoud Parto, Christopher Saldana, Thomas Kurfess, 2020 — *Mahmoud Parto, Christopher Saldana, Thomas Kurfess.* A Novel Three-Layer IoT Architecture for Shared, Private, Scalable, and Real-time Machine Learning from Ubiquitous Cyber-Physical Systems. Procedia Manufacturing, 48. Pp. 959–967. ISSN 2351–9789. https://doi.org/10.1016/j.promfg.2020.05.135 (in Eng.).

Mashal I., Alsaryrah O., Chung T., Yang C., Kuo W., Agrawal D., 2015 — *Mashal I., Alsaryrah O., Chung T., Yang C., Kuo W., Agrawal D.* Choices for interaction with things on Internet and underlying issues. Ad Hoc Netw, 28. Pp. 68–90. (in Eng.).

Nurlan Z., Kokenovna T.Z., Othman M., Adamova A., 2021 — *Nurlan Z., Kokenovna T.Z., Othman M., Adamova A.*, Resource Allocation Approach for Optimal Routing in IoT Wireless Mesh Networks. IEEE Access, 9:153926–153942. doi: 10.1109/ACCESS.2021.3123903. (in Eng.).

Omar S., Masud M., 2013 — *Omar S., Masud M.* Towards Internet of Things: Survey and Future Vision. International Journal of Computer Networks, 5(1): 17. (in Eng.).

Pallavi S., Smruti R.S., 2017 — *Pallavi S., Smruti R.S.* Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017:9324035. https://doi.org/10.1155/2017/9324035. (in Eng.).

Paul B., 2022 — *Paul B.* Internet of Things (IoT), Three-Layer Architecture, Security Issues and Counter Measures. ICT Analysis and Applications, 314. Pp. 23–34. https://doi.org/10.1007/978-981-16-5655-2_3. (in Eng.).

Poschmann A., 2009 — *Poschmann A.* Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. Ph.D. Thesis. Ruhr University Bochum, 2009. (in Eng.).

Prakasam P. et al., 2022 — *Prakasam P. et al.* Low latency, area and optimal power hybrid lightweight cryptography authentication scheme for internet of things applications. Wireless Personal Communications, 126(1). Pp. 351–365. (in Eng.).

Raja G.S., Prabhakar V.S., 2022 — *Raja G.S., Prabhakar V.S.* Intelligent edge based smart farming with LoRa and IoT. International Journal of System Assurance Engineering and Management, 2022. Pp. 1–7. (in Eng.).

Rana Muhammad, Quazi Mamun, Rafiqul Islam, 2022 — *Rana Muhammad, Quazi Mamun, Rafiqul Islam,* Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129. Pp. 77–89. ISSN 0167–739X. https://doi.org/10.1016/j.future.2021.11.011. (in Eng.).

Shannon C.E., 1949 — *Shannon C.E.* Communication theory of secrecy systems. The Bell System Technical Journal, 28(4). Pp. 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x. (in Eng.).

Sheeja S. et al., 2022 — *Sheeja S. et al.* Towards an Optimal Security Using Multifactor Scalable Lightweight Cryptography for IoT. 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4). IEEE, 2022. Pp. 1–6. (in Eng.).

Silva D., Heideker A., Zyrianoff I.D. et al., 2022 — *Silva D., Heideker A., Zyrianoff I.D. et al.* A Management Architecture for IoT Smart Solutions: Design and Implementation. J Netw Syst Manage, 30(35). (in Eng.).

Singh D., Pati B., Panigrahi C., Swagatika S., 2020 — *Singh D., Pati B., Panigrahi C., Swagatika S.* Security Issues in IoT and their Countermeasures. Smart City Applications, 10. (in Eng.).

Singh S., Sharma P.K., Moon S.Y. et al., 2017 — *Singh S., Sharma P.K., Moon S.Y. et al.* Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-017-0494-4. (in Eng.).

Tsantikidou K., Sklavos N., 2022 — *Tsantikidou K., Sklavos N.* Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare. Cryptography, 6(3):45 (in Eng.).

Vermesan O., Friess P., Guillemin P., Gusmeroli S., Sundmaeker H., Bassi A., Jubert I., Mazura M., Harrison M., Eisenhauer M., Doody P., 2009. — *Vermesan O., Friess P., Guillemin P., Gusmeroli S., Sundmaeker H., Bassi A., Jubert I., Mazura M., Harrison M., Eisenhauer M., Doody P.* Internet of Things Strategic Research Roadmap. (in Eng.).

Yildirim Muhammed, Demiroğlu Uğur, Şenol Bilal, 2021 — *Yildirim Muhammed, Demiroğlu Uğur, Şenol Bilal.* An in-depth exam of IoT, IoT Core Components, IoT Layers, and Attack Types. European Journal of Science and Technology. 10.31590/ejosat.1010023 (in Eng.).

Zhong C., Zhu Z., Huang R., 2017 — *Zhong C., Zhu Z., Huang R.* Study on the IOT Architecture and Access Technology. 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, 2017. Pp. 113–116. doi: 10.1109/DCABES.2017.32.(in Eng.).

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

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)

Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 12.06.2023.
Формат 60х881/8. Бумага офсетная. Печать –ризограф.
19,0 п.л. Тираж 300. Заказ 2.

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