REVIEW
of the official reviewer for the dissertation work of
Sakan Kairat Sakanuly on the topic "Development of hashing algorithms based on iterative block ciphers and research of their cryptographic strength", granted for the degree of Doctor of Philosophy (PhD) in the doctoral program "8D06301 – Information Security Systems".

№ p/p	Criteria	Compliance with the criteria (you must mark one of the answer options a)	Substantiation of the position of the official reviewer
1.	The dissertation's topic (as of its approval date) corresponds to the directions of the development of science and/or state programs.	1.1 Compliance with priority areas of science development or state programs: the topic of the dissertation work, "Development of hashing algorithms based on iterative block ciphers and research of their cryptographic strength" corresponds to priority areas of science, such as intelligent systems, artificial intelligence, social research, and information technologies.	The dissertation work corresponds to the priority area of science development of "Information, communication and space technologies" and the Concept of cybersecurity ("Cyber shield of Kazakhstan") approved by the Decree of the Government of the Republic of Kazakhstan dated June 30, 2017, No. 407.
		1) <u>The dissertation was completed within the framework of a project or target program financed from the state budget (indicate the name and number of the project or program)</u> 2) The dissertation was completed within the framework of another state program (indicate the name of the program) 3) The dissertation corresponds to the priority direction of the development of science, approved by the Higher Scientific and Technical Commission under the Government of the Republic of Kazakhstan (indicate the direction)	The dissertation was completed within the framework of the research project funded by the Program Targeted Financing "Development and study of hashing algorithms of arbitrary length for digital signatures and assessment of their security" (2021-2022, state registration number: OR11465439).

2.	Importance for science	The work **makes** / does not make a significant contribution to science, and its importance is well **disclosed** / not disclosed	The obtained results of the dissertation work make a theoretical and practical contribution to the development and creation of cryptographic information protection facilities and systems in Kazakhstan. They can be used to ensure the protection, reliability, and authenticity of information during its exchange and storage in various information and telecommunication systems. In the dissertation work, a new data hashing algorithm based on a new block cipher was developed, which provides a high level of security when searching for collisions and preimages.
3.	The principle of independence	level: **1) High;** 2) Medium; 3) Low; 4) There is no independence	The dissertation author independently substantiated and proved the scientific provisions submitted for defense, and argued the relevance of the research topic. The level of independence of the author of the dissertation work is considered high and consists of reviewing and analyzing literature data, performing the scientific and experimental part of the work, conducting comparative work, presenting a generalization, conclusion, and evaluation of the results obtained.
4.	The principle of internal unity	4.1 Rationale for the relevance of the dissertation : **1) Justified;** 2) Partially justified; 3) Not justified.	The development and research of new approaches to ensuring information security are of high relevance due to the growing need for electronic data exchange in the population and the introduction of innovative technologies in people's daily lives. In Kazakhstan, the security of electronic data is carried out mainly by international cryptographic standards, algorithms, and technical means. Based on this, the creation of domestic information security tools, including cryptographic ones, is considered an urgent and priority area.
		4.2 The content of the dissertation reflects the topic of the dissertation: **1) Reflects;** 2) Partially reflects; 3) Does not reflect	The dissertation introduces a new data hashing algorithm, HBC-256, based on the novel symmetric block cipher algorithm CF. It also presents a security analysis of the proposed algorithm using various cryptographic and statistical methods, as well as an assessment of its efficiency for different implementations.
		4.3. The purpose and objectives correspond to the topic of the dissertation: **1) Correspond;** 2) Partially correspond; 3) Do not match	The main goal and objective of the dissertation work is to develop a secure and high-performance hashing algorithm based on a block cipher, adapted to software and hardware implementation and parallel computing, as well as to study its security and efficiency properties.
		4.4 All sections and provisions of the dissertation are logically interconnected: **1) are fully interconnected;** 2) the relationship is partial; 3) there is no relationship	The dissertation work is a completed scientific study and its content fully reflects the topic of the dissertation. The work structurally consists of an introduction, four sections, a conclusion, and five appendices, which are logically structured and clearly interconnected.

		4.5 New solutions proposed by the author (principles, methods) are argued and evaluated in comparison with known solutions: **1) <u>there is a critical analysis;</u>** 2) partial analysis; 3) the analysis is not one's own opinions, but quotes from other authors	The reliability and relevance of the scientific results, conclusions, and findings are substantiated by the data obtained through the assessment of "near collisions" and the criteria for avalanche/strict avalanche effect, the application of statistical tests and methods of differential, linear, and algebraic cryptographic analysis. Additionally, an evaluation of efficiency was conducted among different implementations and in comparison with other hashing algorithms.
5.	The principle of scientific novelty	5.1 Are scientific results and statements new? **<u>1) completely new;</u>** 2) partially new (25-75% are new); 3) not new (less than 25% are new)	The scientific results of the dissertation are entirely novel. In the course of the dissertation work, the following new scientific approaches have been developed: - A new scheme of conjugate utilizing four 4-bit S-boxes based on the indices of matrix elements has been proposed. The application of this scheme is expected to enhance the security of the algorithm and more efficient use of memory in the hardware implementation of microchips; - A new scheme for the application of nonlinear transformations in the compression function has been proposed, which reduces the number of rounds required; - The possibility of selecting k parts of the hashing block relative to the size of the original input message has been introduced. This, in turn, increases computational efficiency (k=3,…, 8, k is the number of parts).
		5.2 Are the conclusions of the dissertation new? **<u>1) completely new;</u>** 2) partially new (25-75% are new); 3) not new (less than 25% are new)	The results and conclusions are corroborated by the outcomes of computational and statistical experiments conducted on the developed hashing algorithm, which are comprehensively described in the following articles: - Sakan K., Nyssanbayeva S., Kapalova N., Algazy K., Khompysh A., Dyusenbayev D. Development and analysis of the new hashing algorithm based on block cipher // Eastern-European Journal of Enterprise Technologies. Ukraine. – 2022. – № 2/9(116), https://doi.org/10.15587/1729-4061.2022.252060. ***Article-1.*** - Algazy K., Sakan K., Kapalova N., Nyssanbayeva S. and Dyusenbayev D. Differential analysis of a cryptographic hashing algorithm HBC-256 // Appl. Sci. – 2022, 12(19), 10173. https://doi.org/ 10.3390/app121910173. |***Article-2.*** Kunbolat Algazy, Kairat Sakan, Nursulu Kapalova. Evaluation of the strength and performance of a new hashing algorithm based on a block cipher // International Journal of Electrical and Computer Engineering, Vol.13, № 3, June 2023, DOI: http://doi.org/10.11591/ijece.v13i3. ***Article-3.***
		5.3 Technical, technological, economic, or managerial solutions are new and justified: 1) completely new;	During the research, the HBC-256 hashing algorithm was developed, which is adapted for parallel computations and hardware-software implementations. The HBC-256 algorithm allows for the selection of different lengths of the hashing block, each

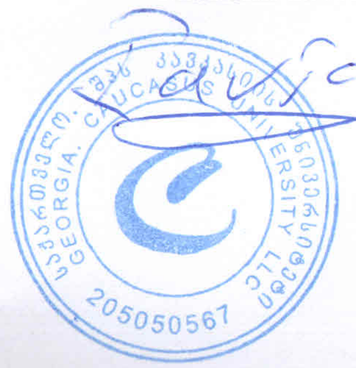
		2) partially new (25-75% are new); 3) not new (less than 25% are new)	composed of 128**k* bits, where *k* can take values from 3 to 8. The Wide-pipe construction and the Davies-Meyer scheme were utilized for data processing. In HBC-256, the symmetric block cipher algorithm CF was proposed as the compression function.
6.	Validity of the main conclusions	All the main conclusions **are based** / not based on scientifically sound evidence or are reasonably well substantiated (for qualitative research and areas of study in the arts and humanities)	The credibility of the obtained scientific results is substantiated through the verification of conducted experiments, as evidenced by publications in reputable international journals with nonzero impact factors according to the Scopus and Web of Science databases. Additionally, the results have been presented at international conferences and scientific seminars organized by foreign higher education institutions and research organizations.
7.	Basic provisions for defense	The following questions need to be answered for each position separately: 7.1 Is the position proven? 1) proven; 2) rather proven; 3) rather unproven; 4) not proven 7.2 Is it trivial? 1) yes; 2) no 7.3 Is it new? 1) yes; 2) no 7.4 Level to apply: 1) narrow; 2) medium; 3) wide; 7.5 Is it proven in the article? 1) yes; 2) no	**Provision 1.** A new hashing algorithm based on a block cipher has been developed, tailored for parallel computing and hardware-software implementation. 7.1 **proven**; 7.2 **no**; 7.3 **yes**; 7.4 **wide**; 7.5 **yes**, in Article-1, *referred to in paragraph 5.2*. **Provision 2.** A novel scheme has been proposed for the conjugate application of four 4-bit S-boxes based on the indices of matrix elements. Its application is expected to enhance the security of the algorithm and make more efficient use of memory in the hardware implementation. 7.1 **proven**; 7.2 **no**; 7.3 **yes**; 7.4 **wide**; 7.5 **yes**, in Article-1, Article-2, Article-3, *referred to in paragraph 5.2*. **Provision 3.** A new scheme for applying a nonlinear transformation in the compression function is proposed, which makes it possible to reduce the number of rounds; 7.1 **proven**; 7.2 **no**; 7.3 **yes**; 7.4 **wide**; 7.5 **yes**, in Article-1, Article-3, *referred to in paragraph 5.2*. **Provision 4.** An option has been introduced to choose *k* parts of the hashing block relative to the size of the original input message. This, in turn, increases computational efficiency (*k*=3,…,8, where *k* is the number of parts). 7.1 **proven**; 7.2 **no**; 7.3 **yes**; 7.4 **wide**; 7.5 **yes**, in Article-1, Article-3, *referred to in paragraph 5.2*.

8.	The principle of certainty Reliability of sources and information provided	8.1 Choice of methodology - justified or methodology described in sufficient detail **1) yes;** 2) no	The work describes in detail the methodology, namely various approaches, constructions, and schemes (PGV functions) for using block ciphers as a compressing function in hashing algorithms. To ensure one-way hashing, the Davis-Meyer scheme was used. The correctness and relevance of the application of the above approaches, designs, and schemes in the HBC-256 algorithm are justified by evaluating the results of the study.
		8.2 The results of the dissertation work were obtained using modern methods of scientific research and methods of processing and interpreting data using computer technologies: **1) yes;** 2) no	The dissertation results were obtained using contemporary scientific research methods, data processing, and interpretation techniques with the aid of computer technologies. Numerical experiments were conducted using the programming languages Delphi-7 and C++. For hardware implementation, the MYIR Z-turn development board was chosen, equipped with 1GB of RAM, a NAND Flash chip with 16MB of memory, and a Cortex A9 microprocessor. The software code for Cortex was written in the C programming language with the use of assembler inserts.
		8.3 Theoretical conclusions, models, identified relationships, and patterns are proven and confirmed by experimental research (for areas of training in pedagogical sciences, the results are proven based on a pedagogical experiment): **1) yes;** 2) no	Sections 3 and 4 of the dissertation work are dedicated to the research on the security, reliability, and efficiency of the developed HBC-256 algorithm. Specifically, these sections focus on irreversibility and resistance to first and second-order collisions, as well as preimage attacks. Assessments of the "avalanche effect" and "strict avalanche effect" of the HBC-256 algorithm and CF were obtained. Statistical properties of encrypted hash values were investigated using a set of NIST and Knuth tests. The cryptographic strength of the CF cipher and the collision resistance of the HBC-256 hashing algorithm are confirmed by the results of differential, linear, and algebraic cryptographic analysis methods.
		8.4 Important statements **are supported** / partially confirmed / not supported by references to the relevant and reliable scientific literature	Important statements are supported by references to current and reliable scientific literature.
		8.5 Used literature sources **are sufficient** / not sufficient for a literature review	The list of used literature includes 99 references in English, Russian, and Kazakh. Among them, there are sources in high-impact foreign publications, which were sufficient for a literary review.
9	Principle of practical value	9.1 The dissertation has a theoretical value: **1) yes;** 2) no	The main advantage of the developed HBC-256 algorithm, built on the basis of a block cipher, is the use of well-studied cryptographic primitives and constructions. During the research work, it was proved that the cryptographic strength of the encryption algorithm used ensures the security and reliability of the hashing algorithm itself. The obtained results are expected to have a positive impact on the development of domestic

			cryptographic systems and information security tools, thereby expanding the approaches for implementing effective data hashing algorithms.
		9.2 The dissertation is of practical importance, and there is a high probability of applying the results obtained in practice: **1) yes;** 2) no	The proposed hashing algorithm, HBC-256, with its security properties and resistance to both first and second-order collisions and preimage attacks, may prove to be highly competitive and find applications in information security for data transmission and storage in general-purpose information and communication systems and networks.
		9.3 Are the suggestions for practice new? **1) completely new;** 2) partially new (25-75% are new); 3) not new (less than 25% are new)	The proposed algorithm can be applied in the development of post-quantum cryptography algorithms based on hash functions. In addition, it can be used to create domestic information security tools in the Republic of Kazakhstan.
10.	Quality of writing and design	Quality of academic writing: **1) high;** 2) average; 3) below average; 4) low.	The dissertation has been prepared in accordance with the specified requirements. The primary information in the work is logically presented, and there are no digressions. The work is characterized by clarity and precision in presenting data, fully adhering to the scientific style and academic presentation of information.

The dissertation work of **Sakan Kairat Sakanuly** on the topic "**Development of hashing algorithms based on iterative block ciphers and research of their cryptographic strength**" complies with the Rules for awarding the degree of Doctor of Philosophy (PhD). Its author Sakan Kairat Sakanuly deserves to be awarded the Doctor of Philosophy (PhD) degree in the doctoral program **"8D06301 – Information Security Systems".**

Official reviewer:
PhD in Mathematics,
Affiliate professor and the Head of cyber security direction at Caucasus University,
President at Scientific Cyber Security Association (SCSA) **Maksim Iavich**



«8D06301 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесіне іздену үшін ұсынылған Сақан Қайрат Сақанұлының «Итерациялық блоктық шифрларға негізделген хеш алгоритмдерін құру және олардың криптоберіктілігін зерттеу» тақырыбындағы диссертациялық жұмысына ресми рецензенттің

СЫН-ПІКІРІ

р/н №	Критерийлер	Критерийлер сәйкестігі	Ресми рецензенттің ұстанымы
1.	Диссертация тақырыбының (бекіту күніне) ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкес болуы	1.1 Ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкестігі: «Итерациялық блоктық шифрларға негізделген хеш алгоритмдерін құру және олардың криптоберіктілігін зерттеу» тақырыбындағы диссертациялық жұмыс интеллектуалды жүйелер, жасанды интеллект, әлеуметтік зерттеулер және ақпараттық технологиялар сияқты ғылымның басым бағыттарына сәйкес келеді.	Диссертациялық жұмыс «Ақпараттық, коммуникациялық және ғарыштық технологиялар» ғылымын дамытудың басым бағытына және Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген Киберқауіпсіздік Тұжырымдамасына («Қазақстанның киберқалқаны») сәйкес келеді.
		1) Диссертация мемлекет бюджетінен қаржыландырылатын жобаның немесе нысаналы бағдарламаның аясында орындалған (жобаның немесе бағдарламаның атауы мен нөмірі); 2) Диссертация басқа мемлекеттік бағдарлама аясында орындалған (бағдарламаның атауы) 3) Диссертация Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылым дамуының басым бағытына сәйкес (бағытын көрсету)	Диссертациялық жұмыс «Цифрлы қолтаңбалар үшін еркін ұзындықтағы хештеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау» бағдарламалы-нысаналы қарржыландыру жобасының ғылыми-зерттеу жұмыстары шеңберінде орындалды (2021-2022 жж., мемлекеттік тіркеу нөмірі: OR11465439).
2.	Ғылымға маңыздылығы	Жұмыс ғылымға елеулі үлесін **қосады**/қоспайды, ал оның маңыздылығы **ашылған**/ашылмаған.	Диссертациялық жұмыстың алынған нәтижелері Қазақстанда ақпаратты криптографиялық қорғау құралдары мен жүйелерін дамытуға және құруға теориялық және тәжірибелің тұрғыдан үлес қосады. Олар әртүрлі ақпараттық-телекоммуникациялық жүйелерде ақпараттың алмасуы және сақталуы кезінде оның қорғалуын, сенімділігі мен түпнұсқалығын қамтамасыз ету мақсатында пайдаланылуы мүмкін. Жұмыста коллизиялар мен алғашқы түпбейнені іздеу кезінде қауіпсіздіктің жоғары деңгейін

			қамтамасыз ететін жаңа блоктық шифр негізінде деректерді хештеудің жаңа алгоритмі жасалды.
3.	Өзі жазу принципі	Өзі жазу деңгейі: **1) жоғары;** 2) орташа; 3) төмен; 4) өзі жазбаған	Диссертант диссертация қорғауға ұсынылған ғылыми ережелерді жеке өзі негіздеген, дәлелдеген, және зерттеу тақырыбының өзектілігін дәлелдеген. Диссертация авторының өз бетімен жұмыс істеу деңгейі жоғары болып саналады және ол әдеби деректерді шолу мен талдаудан, жұмыстың ғылыми және эксперименттік бөлігін орындаудан, салыстырмалы жұмысты жүргізуден, алынған нәтижелерді жалпылау, қорытындылау және бағалаудан көрінеді.
4.	Ішкі бірлік принципі	4.1 Диссертация өзектілігінің негіздемесі: **1) негізделген;** 2) жартылай негізделген; 3) негізделмеген.	Ақпараттық қауіпсіздікті қамтамасыз етудің жаңа тәсілдерін әзірлеу және зерттеу халықтың ақпаратты электрондық алмасу қажеттілігінің өсуіне және адамдардың күнделікті өміріне инновациялық технологияларды енгізуге байланысты жоғары дәрежедегі өзектілікке ие. Қазақстанда электрондық ақпараттың қауіпсіздігін қамтамасыз ету негізінен халықаралық криптографиялық стандарттармен, алгоритмдермен және техникалық құралдармен жүзеге асырылып келеді. Осыған сүйене отырып, ақпаратты криптографиялық тәсілмен қорғаудың отандық құралдарын құру өзекті және басым бағыт болып саналады.
		4.2 Диссертация мазмұны диссертация тақырыбын айқындайды **1) айқындайды;** 2) жартылай айқындайды; 3) айқындамайды	Диссертацияда CF жаңа симметриялы блоктық шифрлау алгоритмі негізінде HBC-256 деректері хештеудің жаңа алгоритмін ұсынады. Жұмыста ұсынылған алгоритмнің қауіпсіздігін криптографиялық және статистикалық талдаудың әртүрлі әдістерімен зерттеу нәтижелері, сондай-ақ оны іске асыру әртүрлеріне қатысты тиімділікті бағалау ұсынылған.
		4.3. Мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді: **1) сәйкес келеді;** 2) жартылай сәйкес келеді; 3) сәйкес келмейді	Диссертациялық жұмыстың негізгі мақсаты мен міндеті блоктық шифр негізінде бағдарламалық-аппараттық іске асыруға және параллельді есептеулерге бейімделген, қауіпсіз және өнімділігі жағынан жоғары хештеу алгоритмін әзірлеу, сондай-ақ оның қауіпсіздік және тиімділік қасиеттерін зерттеу болып табылады.
		4.4. Диссертацияның барлық бөлімдері мен құрылысы логикалық байланысқан: **1) толық байланысқан;** 2) жартылай байланысқан; 3) байланыс жоқ	Диссертациялық жұмыс аяқталған ғылыми зерттеу болып табылады және оның мазмұны диссертация тақырыбына толық сәйкес келеді. Жұмыс құрылымдық жағынан бір-бірімен логикалық нақты байланысқан кіріспеден, төрт бөлімнен, қорытындыдан және бес қосымшадан тұрады.
		4.5 Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған: **1) сыни талдау бар;**	Ғылыми нәтиженің дұрыстығы мен өзектілігі «жақын коллизияларды» және лавиндік әсер / қатаң лавиндік әсер критерийлерін бағалау, статистикалық сынақтар мен дифференциалды, сызықтық және алгебралық криптографиялық талдау әдістерін қолдану нәтижесінде алынған мәліметтермен негізделеді. Сонымен қатар, іске асыру түрлері

ПАРАҚТЫҢ АРҒЫ ЖАҒЫНА ҚАРАҢЫЗ
СМ. НА ОБОРОТНОЙ СТОРОНЕ

		2) талдау жартылай жүргізілген; 3) талдау өз пікірін емес, басқа авторлардың еңбектеріне негізделген	арасында, сондай-ақ басқа хештеу алгоритмдерімен салыстыру кезінде тиімділікті бағалау жүргізілген.
5.	Ғылыми жаңашылдық принципі	5.1 Ғылыми нәтижелер мен қағидаттар жаңа болып табыла ма? **1) толығымен жаңа;** 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Диссертацияның ғылыми нәтижелері толықтай жаңа. Диссертациялық жұмысты орындау барысында келесі жаңа ғылыми тәсілдер әзірленді: - матрица элементінің индекстеріне қатысты төрт 4-биттік S-блоктарды біріктіріп қолданудың жаңа схемасы ұсынылды, оны қолдану алгоритмнің қауіпсіздігін арттыруға және аппараттық құралдарды іске асыруда микросхеманың жадын тиімдірек пайдалануға мүмкіндік береді; - сызықтық емес түрлендіруді қысу функциясында қолданудың жаңа схемасы ұсынылған, бұл раундтардың санын азайтуға мүмкіндік береді; - бастапқы хештелген хабарламаның өлшеміне қатысты хештеу блогының k бөліктерін таңдау мүмкіндігі ұсынылады, бұл өз кезегінде есептеу өнімділігін арттырады (k=3,..., 8, k – бөліктер саны).
		5.2 Диссертацияның қорытындылары жаңа болып табыла ма? **1) толығымен жаңа;** 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Нәтижелер мен тұжырымдар әзірленген хештеу алгоритмі бойынша төменгі мақалаларда егжей-тегжейлі сипатталып, онда есептеу және статистикалық тәжірибелердің нәтижелерімен расталады: - Sakan K., Nyssanbayeva S., Kapalova N., Algazy K., Khompysh A., Dyusenbayev D. Development and analysis of the new hashing algorithm based on block cipher // Eastern-European Journal of Enterprise Technologies. Ukraine. – 2022. – № 2/9(116), https://doi.org/10.15587/1729-4061.2022.252060. ***Мақала -1.*** - Algazy K., Sakan K., Kapalova N., Nyssanbayeva S. and Dyusenbayev D. Differential analysis of a cryptographic hashing algorithm HBC-256 // Appl. Sci. – 2022, 12(19), 10173. https://doi.org/ 10.3390/app121910173. ***Мақала - 2.*** - Kunbolat Algazy, Kairat Sakan, Nursulu Kapalova. Evaluation of the strength and performance of a new hashing algorithm based on a block cipher // International Journal of Electrical and Computer Engineering, Vol.13, № 3, June 2023, DOI: http://doi.org/10.11591/ijece.v13i3. ***Мақала-3.***
		5.3 Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген бе? 1) толығымен жаңа; **2) жартылай жаңа (25-75% жаңа болып табылады);** 3) жаңа емес (25% кем жаңа болып табылады)	Жұмыс барысында параллельді есептеулер мен бағдарламалық-аппараттық іске асыруға бейімделген жаңа HBC-256 хештеу алгоритмі әзірленді. HBC-256 алгоритмі хештелетін блоктың әртүрлі 128*k биттік ұзындығын таңдауға мүмкіндік береді, мұнда k 3-тен 8-ге дейінгі мәндерді қабылдай алады. Деректерді өңдеу үшін Wide-pipe құрылымы және Девиса-Мейер схемасы қолданылды. HBC-256-да қысу функциясы ретінде симметриялы CF блоктық шифрлау алгоритмі жасалып ұсынылды.

6.	Негізгі қорытындыларды ң негізділігі	Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде **негізделген**/негізделмеген (qualitative research және өнертану және гуманитарлық бағыттары боынша)	Алынған ғылыми нәтижелердің ақиқаттығы жүргізілген эксперименттердің Scopus және Web of Science дерекқорындағы нөлдік емес импакт-факторы бар рейтингтік халықаралық журналдарда жариялау арқылы, сондай-ақ шетелдік жоғары оқу орындары мен ғылыми ұйымдарында ұйымдастырылған халықаралық конференциялар мен ғылыми семинарлардағы жасалған баяндамалармен негізделеді.
7.	Қорғауға шығарылған негізгі қағидаттар	Әр қағидат бойынша келесі сұрақтарға жауап беру қажет: 7.1 Қағидат дәлелденді ме? 1) дәлелденді; 2) шамамен дәлелденді; 3) шамамен дәлелденбеді; 4) дәлелденбеді 7.2 Тривиалды ма? 1) ия; 2) жоқ 7.3 Жаңа ма? 1) ия; 2) жоқ 7.4 Қолдану деңгейі: 1) тар; 2) орташа; 3) кең 7.5 Мақалада дәлелденген бе? 1) ия; 2) жоқ	**Қағидат-1:** Параллельді есептеулер мен бағдарламалық-аппараттық іске асыруға бейімделген блоктық шифр негізінде жаңа хештеу алгоритмі әзірленді; 7.1 **дәлелденді**; 7.2 **жоқ**; 7.3 **иә**; 7.4 **кең**; 7.5 **иә**, 5.2 бөлімдегі Мақала-1-мен дәлелденген. **Қағидат-2:** Матрица элементінің индекстеріне қатысты төрт 4 биттік S-блоктарды біріктіріп қолданудың жаңа схемасы ұсынылды, оны қолдану алгоритмнің қауіпсіздігін арттырады және аппараттық құралдарды іске асыруда микросхеманың жадын тиімді пайдаланады; 7.1 **дәлелденді**; 7.2 **жоқ**; 7.3 **иә**; 7.4 **кең**; 7.5 **иә**, 5.2 бөлімдегі Мақала-1, Мақала-2, Мақала-3-пен дәлелденген. **Қағидат-3:** Сызықтық емес түрлендіруді қысу функциясына қолданудың жаңа схемасы ұсынылған, бұл раундтардың санын азайтуға мүмкіндік береді; 7.1 **дәлелденді**; 7.2 **жоқ**; 7.3 **иә**; 7.4 **кең**; 7.5 **иә**, 5.2 бөлімдегі Мақала-1, Мақала-3-пен дәлелденген. **Қағидат-4:** Бастапқы хештелетін хабарламаның өлшеміне қатысты хештеу блогының k бөліктерін таңдау мүмкіндігі ұсынылды, бұл өз кезегінде есептеу өнімділігін арттырады (k=3,..., 8, k – бөліктер саны). 7.1 **дәлелденді**; 7.2 **жоқ**; 7.3 **иә**; 7.4 **кең**; 7.5 **иә**, 5.2 бөлімдегі Мақала-1, Мақала-3-пен дәлелденген.
8.	Дәйектілік принципі Дереккөздер мен ұсынылған ақпараттың дәйектілігі	8.1 Әдістеменің таңдауы - негізделген немесе әдіснама нақты жазылған 1) **ия;** 2) жоқ	Жұмыста хештеу алгоритмдерінде қысу функциясы ретінде блоктық шифрларды қолданудың әртүрлі тәсілдері, конструкциялары мен схемалары (PGV функциялары) егжей-тегжейлі сипатталған. Хештеудің бірбағыттылығын қамтамасыз ету үшін Девис-Мейер схемасы қолданылды. HBC-256 алгоритміндегі жоғарыда аталған тәсілдерді, конструкциялар мен сұлбаларды қолданудың дұрыстығы мен өзектілігі зерттеу нәтижелерін бағалауда көрсетілген.

		8.2 Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған: 1) **ия;** 2) жоқ	Диссертацияның нәтижелері компьютерлік технологияларды қолдана отырып, сондай-ақ деректерді ғылыми зерттеудің, өңдеудің және түсіндірудің заманауи әдістерін қолдана отырып алынды. Сандық эксперименттер Delphi-7 және C бағдарламалау тілдері арқылы алынған. Аппараттық құралдарды іске асыру үшін 1 ГБ жедел жадысы мен 16 Мб жады бар NAND Flash микросхемасы және Cortex A9 микропроцессоры бар MIR Z-turn тақташасы таңдалды. Cortex үшін ассемблер бағдарламалық кодын кірістіре отырып, C бағдарламалау тілінде орындалған.
		8.3 Теориялық қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар эксперименттік зерттеулермен дәлелденген және расталған (педагогикалық ғылымдар бойынша даярлау бағыттары үшін нәтижелер педагогикалық эксперимент негізінде дәлелденеді): 1) **ия;** 2) жоқ	Статистические свойства зашифрованных хеш-значений исследовались с использованием набора тестов NIST и Кнута. Криптостойкость шифра CF и устойчивость к коллизиям алгоритма хеширования HBC-256 подтверждается результатами методов дифференциального, линейного и алгебраического криптографического анализа. Диссертацияның 3 және 4-бөлімдері HBC-256 алгоритмінің қауіпсіздігі, сенімділігі мен тиімділігін, атап айтқанда, бірінші және екінші типтегі коллизияны іздеу, алғашқы түпбейнеге қатысты қайтымсыздық пен төзімділікті зерттеуге арналған. HBC-256 және CF алгоритмінің «лавиндік әсерге» / «қатаң лавиндік әсерлерге» қатысты зерттеулердің бағалары алынды. Шифрланған хеш-мәндерінің статистикалық қасиеттері NIST және Д. Кнуттың сынақтар жиынтығы көмегімен зерттелді. CF шифрының криптоберіктілігі және HBC-256 хештеу алгоритмінің коллизияға төзімділігі дифференциалды, сызықтық және алгебралық криптографиялық талдау әдістерінің нәтижелерімен расталған.
		8.4 Маңызды мәлімдемелер нақты және сенімді ғылыми әдебиеттерге сілтемелермен **расталған** / ішінара расталған / расталмаған	Маңызды мәлімдемелер маңызды және сенімді ғылыми әдебиеттерге сілтемелер жасау арқылы расталған.
		8.5 Пайдаланылған әдебиеттер тізімі әдеби шолуға **жеткілікті**/жеткіліксіз	Пайдаланылған әдебиеттер тізіміне ағылшын, орыс және қазақ тілдеріндегі 99 сілтеме кіреді. Олардың ішінде әдеби шолу жүргізуге жеткілікті жоғары рейтингі бар шетелдік басылымдардағы дереккөздер де бар.
9	Практикалық құндылық принципі	9.1 Диссертацияның теориялық маңызы бар: 1) **ия;** 2) жоқ	Блоктық шифр негізінде жасалған HBC-256 алгоритмінің басты артықшылығы – жақсы зерттелген криптографиялық примитивтер мен конструкцияларды пайдалану болып саналады. Зерттеу жұмыстары барысында қолданылатын шифрлау алгоритмінің криптографиялық беріктігі хештеу алгоритмінің қауіпсіздігі мен сенімділігін қамтамасыз ететіндігі дәлелденді. Алынған нәтижелер болашақта отандық

			криптографиялық жүйелер мен ақпаратты қорғау құралдарының дамуына оң әсер етеді, осылайша деректерді хэштеудің тиімді алгоритмдерін енгізу тәсілдерін кеңейтеді.
		9.2 Диссертацияның практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары: 1) **ия**; 2) жоқ	Ұсынылған HBC-256 хештеу алгоритмі қауіпсіздікті қамтамасыз ету қасиеттері мен бірінші және екінші типтегі коллизиялар мен хеш-мәндерінің түпбейнесін табуға қарсы тұру қасиеттері бойынша бәсекеге қабілетті болуы мүмкін және ақпаратты қорғау үшін ақпараттық-коммуникациялық жүйелерде және жалпы мақсаттағы желілерде тасымалдау және сақтау кезінде қолдануға болады.
		9.3 Практикалық ұсыныстар жаңа болып табылады? 1) **толығымен жаңа;** 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Ұсынылған алгоритм хеш функцияларына негізделген постквантты криптографиялық алгоритмдерді әзірлеу кезінде қолдануға болады. Бұдан басқа, ол Қазақстан Республикасында ақпаратты қорғаудың отандық құралдарын жасау үшін пайдаланылуы мүмкін.
10.	Жазу және ресімдеу сапасы	Академиялық жазу сапасы: 1) **жоғары;** 2) орташа; 3) орташадан төмен; 4) төмен.	Диссертация қойылатын талаптарға сәйкес дайындалған. Жұмыстағы негізгі ақпарат логикалық түсінікті түрде берілген, кеңістіктік шегіністер жоқ. Жұмыс ақпараттарды ұсынудың анықтығы мен дәлдігімен сипатталады, ғылыми стиль мен ақпараттың академиялық сипаттағы жазбасы толығымен сақталған.

Сақан Қайрат Сақанұлының «**Итерациялық блоктық шифрларға негізделген хеш алгоритмдерін құру және олардың криптобериктілігін зерттеу»** тақырыбындағы диссертациялық жұмысы философия докторы (PhD) ғылыми дәрежесін беру ережелеріне сәйкес келеді. Жұмыстың авторы Сақан Қайрат Сақанұлы "**8D06301** – Ақпараттық қауіпсіздік жүйелері" білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін алуға лайық.

Ресми рецензент:
Математика бойынша PhD,
Кавказ Университетінің Киберқауіпсіздік бағытының жетекшісі және профессоры,
Киберқауіпсіздік ғылыми қауымдастығының президенті Максим Явич

ПАРАҚТЫҢ АРҒЫ ЖАҒЫНА ҚАРАҢЫЗ
СМ. НА ОБОРОТНОЙ СТОРОНЕ

Қазақстан Республикасы, Алматы қаласы, екі мың жиырма үшінші жыл, он сегізінші қыркүйек. Құжаттың ағылшын тілінен қазақ тіліне мәтін-аудармасын орындаған аудармашы Белхожаева Аружан Ержанқызы, 20.06.2000 жылы туған, ЖСН 000620601345.

Қолы

Қазақстан Республикасы, Алматы қаласы, екі мың жиырма үшінші жыл, он сегізінші қыркүйек. Қазақстан Республикасы, Алматы қаласы Әділет Министрлігінің халыққа құқықтық көмек және заңгерлік қызмет көрсетуді ұйымдастыру комитетінде, 20.01.2006 жылы берілген № 0000354 лицензиясы негізінде әрекет ететін, мен нотариус Кан Елизавета Герасимовна, аудармашы Белхожаева Аружан Ержанқызының қойылған қолының түпнұсқалығын растаймын. Аудармашының тұлғалығы анықталды, қабілеті мен өкілеттігі тексерілді.

Тіркеу нөмірі № 35857
104 теңге төленді

Нотариус _____
Кан Елизавета Герасимовна

БАЙЛАНЫП ТІГІЛГЕН ЖӘНЕ НӨМІРЛЕНГЕН
ҚҰЖАТ 2 (екі) ПАРАҚТЫ ТҰРАДЫ
ПРОШНУРОВАНО, ПРОНУМЕРОВАНО
НА 2 (двух) ЛИСТАХ

ES730130923091814312 7T28383E

Нотариаттық іс-әрекеттің бірегей нөмірі / Уникальный номер нотариального действия