СПИСОК НАУЧНЫХ ТРУДОВ

АЛҒАЗЫ КҮНБОЛАТ ТІЛЕУХАНҰЛЫ

ORCID ID: 0000-0003-3670-2170
Author ID в Scopus: 57202761698
Author ID в Web of Science: AAH-3846-2021 (GMC-3492-2022)
h-индекс в Scopus: 5
h-индекс в Web of Science: 3

№ п/п	Название публикации	Тип публикации (статья, обзор и т.д.)	Наименование журнала, год публикации (согласно базам данных), DOI	Импакт-фактор журнала, квартиль и область науки* по данным Journal Citation Reports (Жорнал Цитэйшэн Репортс) за год публикации	Индекс в базе данных Web of Science Core Collection (Веб оф Сайенс Кор Коллекшн)	CiteScore (СайтСкор) журнала, процентильи область науки* по данным Scopus (Скопус) за год публикации	ФИО авторов (подчеркнуть ФИО претендента)	Роль претендента (соавтор, первый автор или автор для корреспонденции)
1	Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information	Article	Cogent Engineering, No 9:1, (2022) PP. 1-14, https://doi.org/10.1080/23311916.2022.2080623	IF 1.9, Q2, Computer Science		CiteScore 3.2, Прцентиль - 60, Computer Science (General Computer Science)	Ardabek Khompysh, Nursulu Kapalova, **Kunbolat Algazy**, Dilmukhanbet Dyusenbayev & Kairat Sakan	Автор для корреспонденции

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**

2	Differential Analysis of a Cryptographic Hashing Algorithm HBC-256	Article	Applied Scinces, 2022, 12(19), 10173, - PP 1-16 https://doi.org/10.3390/app121910173	IF 2.7, Q2, Computer Science		CiteScore 4.5, Прцентиль - 63, Computer Science (Computer Science Applications)	**Kunbolat Algazy**, Kairat Sakan, Nursulu Kapalova, Saule Nyssanbayeva and Dilmukhanbet Dyusenbayev	Первый автор
3	Development and study of an encryption algorithm	Article	Computation 2022, 10, 198 - PP 1-16. https://doi.org/10.3390/computation10110198	IF 2.2, Q2, Computer Science		CiteScore 3.3, Прцентиль - 61, Computer Science (General Computer Science)	Kapalova N., Sakan K. **Algazy K.** and Dyusenbayev D.	Автор для корреспонденции
4	Evaluation of the strength and performance of a new hashing algorithm based on a block cipher	Article	International Journal of Electrical and Computer Engineering (IJECE), Vol. 13, No. 3, June 2023, pp. 3124-3130, http://doi.org/10.11591/ijece.v13i3.pp3124-3130			CiteScore 3.8, Прцентиль - 65, Computer Science (General Computer Science)	**Kunbolat Algazy**, Kairat Sakan, Nursulu Kapalova	Первый автор
5	Statistical analysis of the key scheduling of the new lightweight block cipher	Article	International Journal of Electrical and Computer Engineering (IJECE), Vol. 13, No. 6, December 2023, pp. 6817-6826 http://doi.org/10.11591/ijece.v13i6.pp6817-6826			CiteScore 4.1, Прцентиль - 66, Computer Science (General Computer Science)	Nursulu Kapalova, **Kunbolat Algazy**, Armanbek Haumen, Kairat Sakan	Автор для корреспонденции

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**

6	Development and analysis of the new hashing algorithm based on block cipher	Article	Eastern-European Journal of Enterprise Technologies, No 2/9 (116), 2022, - P. 60-73. http://doi.org/10.15587/1729-4061.2022.252060			CiteScore 2.1, Прцентиль - 47, Mathematics (Applied Mathematics)	Kairat Sakan, Saule Nyssanbayeva, Nursulu Kapalova, **Kunbolat Algazy**, Ardabek Khompysh, Dilmukhanbet Dyusenbayev	Автор для корреспонденции
7	Development of a new lightweight encryption algorithm	Article	Eastern-European Journal of Enterprise Technologies, 3(9 (123), 2023, PP. 6–19. https://doi.org/10.15587/1729-4061.2023.280055			CiteScore 2.0, Прцентиль - 45, Mathematics (Applied Mathematics)	Nursulu Kapalova, **Kunbolat Algazy**, Armanbek Haumen	Соавтор
8	CF блокты шифрлау алгоритмі және оны биттік шашырау эффектіне зерттеу	Статья	Хабаршы ЕНУ – Нұрсұлтан, 2022. – № 1. – 6-22 б. DOI: https://doi.org/10.32523/2616-7182/bulmathenu.2022/1.1				С.Е.Нысанбаева, **Қ.Т.Алғазы**, Қ.С.Сақан, А.Хомпыш, Д.С.Дүйсенбаев	Соавтор
9	Study of the cryptographic strength of the s-box obtained on the basis of exponentiation modulo	Статья	Scientific Journal of Astana IT University,2022, volum 12(12), PP. 1–8. DOI: 10.37943/12DZLQ4553				Ardabek Khompysh, Nursulu Kapalova, **Kunbolat Algazy**, Kairat Sakan	Соавтор

Автор **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК **Усатова О.А.**

10	Statistical properties of the pseudorandom sequence generation algorithm	Статья	Scientific Journal of Astana IT University, 18, 2024, pp. 107–119. https://doi.org/10.37943/18LYCW2723				Khompysh A., **Algazy K.**, Kapalova N., Sakan K., & Dyusenbayev D.	Автор для корреспонденции
11	Многоразовая схема пост-квантовой подписи на основе хеша	Статья	Вестник КазАТК №4, 2024г., - стр. 171-180. DOI 10.52167/1609-1817-2024-133-4-171-180				К.С.Сакан, **К.Т.Алгазы**, А.Хомпыш, А.Хаумен	Автор для корреспонденции
12	Модификация алгоритма шифрования «AL01»	Статья	Вестник АУЭС №1, 2022г., - стр.162-170. https://doi.org/10.51775/2790-0886_2022_56_1_162				**Алгазы К.**, Капалова Н.А., Сакан К.С., Хомпыш А.	Первый автор
13	Жаңа 4 биттік S-блок алу әдісі және алынған S-блокты қатал лавиндік критерийі бойынша зерттеу	Статья	Университет еңбектері КарТУ – Қарағанды, 2022. – № 4(89) – 411-417 б. DOI 10.52209/1609-1825_2022_4_411				Хомпыш А., Капалова Н.А., Сакан К.С., Дюсенбаев Д.С., **Алгазы К.Т.**	Соавтор
14	Оценка алгоритма генерации раундовых ключей легковесного шифра LBC-3	Статья	Вестник АУЭС №2, 2023 г., - стр. 66-81. DOI 10.51775/2790-0886_2023_61_2_66				Капалова Н.А., Хаумен А., **Алгазы К.Т.**	Соавтор

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**

15	Линейный криптоанализ алгоритма LBC	Статья	Труды Университета КарТУ – Қараганды, 2023. – № 4(93) – 472-477 с. DOI 10.52209/1609-1825_2023_4_472				**Алгазы К.Т.,** Хаумен А., Хомпыш А., Сакан К.С.	Первый автор
16	Постквантовая цифровая подпись Syrga-1	Статья	Вестник АУЭС №1, 2024г., - стр. 5-15. https://doi.org/10.51775/2790-0886_2024_64_1_5				**К.Т. Алгазы**, К.С. Сакан, А. Хомпыш, Д.С. Дюсенбаев	Первый автор
17	Investigation of the statistical security of a pseudo-random sequence generator	Статья	Proceedings of the XIII International Conference, 2022 September 6-10, Minsk, – P. 137-143.				Nysanbayeva S.E., Kapalova N.A., Dyusenbayev D.S., **Algazy K.T.**	Соавтор
18	Post-quantum cryptography based on hash functions	Статья	Сборник трудов XV Международной научно-практической конференции имени Олега Борисовича Макаревича, Таганрог, Росия 11–15 сентября 2024. – С. 251-258.				**K.T. Algazy**, K.S. Sakan, N.A. Kapalova	Первый автор
19	Дифференциальный криптоанализ легковесного алгоритма LBC	Статья	Материалы II Международной научной конференции «Теоретическая и прикладная криптография». – Минск, 19-20 октября 2023. – С. 94-106.				Н.А. Капалова, **К.Т. Алгазы**, А. Хаумен	Соавтор

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**

20	Реализация квантово-устойчивого криптографического алгоритма HORS с хеш-функцией HAS01-256	Статья	Матер. VIII междунар. науч.-практ. конф. "Информатика и прикладная математика". – Алматы, 2023. – С. 259-264.				Лизунов О.А., **Алгазы К.Т.**	Соавтор
21	Блоктық шифрлау алгоритмін құру және оған позициялы емес полиномдық санау жүйесін қолдану	Монография	ҚР ҒК ҒЖБМ Ақпараттық және есептеуіш технологиялар институтының Ғылыми кеңесінде бекітілген (№15 хаттама, 18.11.2024 ж.) ISBN 978-601-08-4658-6 Алматы, «Дарын баспасы», 2024 – 140 б. (көлемі 8.8 б.т.)				**Алгазы К.Т.**	Единолично
22	Программа «Sandyq-LBC v 3.0»;	Авторское свидетельства	РГП «Национальный институт интеллектуальной собственности» МЮ РК, опубл. 15.08.2023. – 1 с.				Хаумен А., Капалова Н.А., **Алғазы К.Т.**	Соавтор
23	Программа постквантового алгоритма ЭЦП «SYRGA-2»	Авторское свидетельства	РГП «Национальный институт интеллектуальной собственности» МЮ РК, опубл. 02.09.2024. – 1 с.				Лизунов О.А., Сақан Қ.С., **Алғазы К.Т.**, Варенников А.В.	Соавтор

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**

24	Устройство хеширования цифровых данных	Патент	РГП «Национальный институт интеллектуальной собственности» МЮ РК, Патент на полезную модель № 7171 от 03.06.2022.				**Алгазы К.Т.**, Варенников А.В., Васильев И.В., Глухих А.В., Дюсенбаев Д.С., Сакан К.С.	Первый автор

Автор _____ **Алғазы К.Т.**

Ученый секретарь ИИВТ КН МНВО РК _____ **Усатова О.А.**