Приложение 2
к Правилам присвоения ученых званий
(ассоциированный профессор (доцент), профессор)

СПИСОК НАУЧНЫХ ТРУДОВ
САҚАН ҚАЙРАТ САҚАНҰЛЫ

ORCID ID: 0000-0002-6812-6000
Author ID в Scopus: 57687675800
Author ID в Web of Science: AIF-1679-2022
h-индекс в Scopus: 6,
h-индекс в Web of Science: 4

№ 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 за год публикации	Индекс в базе данных Web of Science Core Collection	CiteScore журнала, процентиль и область науки* по данным Scopus за год публикации	ФИО авторов (подчеркнуть ФИО претендента)	Роль претендента (соавтор, первый автор или автор для корреспонденции)
1	Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1	Статья	Computers, 2024, 13(1), 26, pp. 1-14, https://doi.org/10.3390/computers13010026	IF 4.2, Q2, Computer Science	ESCI	CiteScore 7.5, Процентиль -80, Computer Science (Computer Networks and Communications)	Kunbolat Algazy, **Kairat Sakan**, Ardabek Khompysh, Dilmukhanbet Dyusenbayev.	Автор для корреспонденции
2	Syrga2: Post-Quantum Hash-Based Signature Scheme	Статья	Computation, 2024, 12(6), 125, pp. 1-17, https://doi.org/10.3390/computation12060125	IF 1.9, Q2, Mathematics, interdisciplinary applications	ESCI	CiteScore 4.1, Процентиль -61, Computer Science (General Computer Science)	Kunbolat Algazy, **Kairat Sakan,** Saule Nyssanbayeva, Oleg Lizunov.	Автор для корреспонденции

Автор **Сақан Қ.С.**

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

3	Polynomial Commitment in a Verkle Tree Based on a Non-Positional Polynomial Notation	Статья	Computers, Materials & Continua, 2025, vol.84, No.1, pp.1581–1595, https://doi.org/10.32604/cmc.2025.065085.	IF 2.4, Q3, Computer science	SCIE	CiteScore 6.6, Процентиль -73, Computer Science (Computer Science Applications)	Kunbolat Algazy, **Kairat Sakan**, Saule Nyssanbayeva, Ardabek Khompysh.	Автор для корреспонденции
4	Lightweight Hash Function Design for the Internet of Things: Structure and SAT-Based Cryptanalysis	Статья	Algorithms, 2025, 18, 550, pp. 1-20. https://doi.org/10.3390/a18090550.	IF 2.6, Q2, Computer science	ESCI	CiteScore 5.4, Процентиль -77, Computer Science (Computational Theory and Mathematics)	**Kairat Sakan,** Kunbolat Algazy, Nursulu Kapalova and Andrey Varennikov.	Первый автор
5	Efficient Lattice-Based Digital Signatures for Embedded IoT Systems	Статья	Symmetry, 2025, 17(9), 1522, https://doi.org/10.3390/sym17091522.	IF 2.2, Q2, Multidisciplinary sciences	SCIE	CiteScore 5.2, Процентиль -65, Computer Science (Computer Science (miscellaneous))	Maksim Iavich , Nursulu Kapalova, **Kairat Sakan.**	Автор для корреспонденции
6	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.	Первый автор
7	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.	Соавтор

Автор **Сақан Қ.С.**

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

8	«EM chiper» блокты шифрлау алгоритмінің криптоберіктілігін зерттеу	Статья	Вестник Академии гражданской авиации №3, 2025г., Раздел: Компьютерные науки, приборостроение и автоматизация. Стр. 82-93. https://doi.org/10.53364/24138614_2025_38_3_7.				А.Хомпыш **Қ.С.Сақан,** К.Алғазы, А.Ж.Абишева.	Автор для корреспонденции
9	Verkle ағашына векторлық міндеттемелерді құрудың жаңа жолы	Статья	Вестник КазУТБ, Раздел: информационно-коммуникационные и химические технологии, №3, 2025г., стр. 104-116, https://doi.org/10.58805/kazutb.v.3.28-928.				К.Т. Алғазы, **Қ.С. Сақан,** Н.А. Капалова, Е.Ж. Алимжан.	Автор для корреспонденции
10	Диффузионные свойства алгоритма «LWH»	Статья	Вестник КазАТК, Раздел: Автоматизация, телемеханика, связь, компьютерные науки, №6, 2025г., стр. 122-132, https://doi.org/10.52167/1609-1817-2025-141-6-122-132.				Е.Ж. Алимжан., К.Т. Алғазы, **Қ.С. Сақан,** А. Хомпыш.	Соавтор

Автор **Сақан Қ.С.**

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

11	Сызықсыз түйін S-блок үшін изоморфты S-блокты алу әдістері және оларға салыстырмалы криптографиялық талдаулар жүргізу	Статья	ҚазККА хабаршысы, № 142(1), 2026 г., стр. 1-12 б. https://vestnik.alt.edu.kz/index.php/journal/article/view/3085. https://doi.org/10.52167/1609-1817-2026-142-1-371-382.				Турсынова А., **Сақан Қ.,** Алғазы К.	Соавтор
12	Verkle ағаштарына арналған торлық векторлық міндеттемелер	Статья	Academic scientific journal of computer science, № 2 (358), 2026 ж., 67-86 б., https://doi.org/10.32014/2026.2518-1726.427.				Алғазы К.Т., Әлімжан Е.Ж., **Сақан Қ.С.,** Нысанбаева С.Е.	Соавтор
13	Verkle ағашына негізделген цифрлық қолтаңбаның тиімділігін бағалау және салыстырмалы талдау жүргізу	Статья	Азаматтық авиация академиясының Жаршысы, №2, 2026 ж., 148-165 б., https://doi.org/10.53364/24138614_2026_41_2_11.				**Қ.С. Сақан,** К.Т. Алғазы, А.В. Варенников, А.Ж. Абишева.	Первый автор
14	Линейный криптоанализ алгоритма LBC	Статья	Труды Университета КарТУ, Караганды, 2023г. Раздел «Автоматика. Энергетика. ИКТ». – № 4(93) – стр. 472-477. DOI 10.52209/1609-1825_2023_4_472				Алгазы К.Т., Хаумен А., Хомпыш А., **Сакан К.С.**	Соавтор

Автор **Сақан Қ.С.**

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

15	Постквантовая цифровая подпись Syrga-1	Статья	Вестник АУЭС №1, 2024г., Раздел: Информационные, телекоммуникационные и космические технологии. – 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.	Соавтор
16	A new digital signature scheme based on the Verkle tree using the Chinese remainder theorem.	Статья	Proc. SPIE 14009, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2025, 140091H (30 December 2025), https://doi.org/10.1117/12.3099534.				Kunbolat Algazy, **Kairat Sakan,** Daniel Sawicki.	Автор для корреспонденции
17	Application of satisfiability problem solvers for assessing the strength of hash algorithms	Статья	International Journal of Electrical and Computer Engineering, V.15, No.3, June 2025, pp. 3191-3201, DOI: 10.11591/ijece.v15i3.pp3191-3201.				Kunbolat Algazy, **Kairat Sakan,** Andrey Varennikov, Nursulu Kapalova.	Автор для корреспонденции

Автор **Сакан К.С.**

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

18	Post-quantum cryptography based on hash functions	Статья	Сборник трудов XV Междун. научно-практ. конф. 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	Заманауи шифрлау алгоритмдеріндегі s-box қасиеттері мен оларға қойылатын жалпы талаптар	Статья	Матер. X междунар. науч.-практ. конф. "Информатика и прикладная математика". – Алматы, 2025. – С. 382-388.				Ә.Ғ. Тұрсынова, **Қ.С. Сақан.**	Соавтор
20	Разработка схемы постквантовой цифровой подписи на основе хеш-функций и исследование их криптостойкости	Монография	Утверждена Ученым советом Института информационных и вычислительных технологий КН МНВО (Протокол №2 от 27 февраля 2026 г). – Алматы: Дарын, 2026. – 154 с. ISBN 978-601-382-407-9. Объем 9,62 п.л., тираж 500 экз.				**Сақан Қ.С.**	Единолично
21	Способ постквантовой цифровой подписи на основе хеширования	Патент	РГП «Национальный институт интеллектуальной собственности» МЮ РК. Патент на изобретение №38192 от 30.10.2026.				Капалова Н.А., **Сақан Қ.С.,** Алғазы К.Т., Варенников А.В.	Соавтор

Автор _____ **Сақан К.С.**

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

22	Система и способ обеспечения защиты данных устройств интернета вещей	Патент	РГП «Национальный институт интеллектуальной собственности» МЮ РК. Патент на изобретение №38227 от 28.08.2026.				Капалова Н.А., Васильев И.В., Вязигин С.В., Алғазы К.Т. **Сақан Қ.С.**	Соавтор
23	Интеллектуальная система уличного светодиодного освещения	Патент	РГП «Национальный институт интеллектуальной собственности» МЮ РК. Патент на полезную модель. №11096 от 05.09.2025.				Тургынбеков Е.С., Джунисбеков М.Ш., **Сақан Қ.С.,** Кунелбаев М.М.	Соавтор
24	Программный комплекс для создания и верификации криптографических векторных обязательств на основе НПСС (VCNPSS v1.0)	Авторское свидетельства	РГП «Национальный институт интеллектуальной собственности» МЮ РК, 14. А.с. №68294. опубл. 04.03.2026. – 1 с.				Варенников А.В., Нысанбаева С.Е., Алгазы К.Т., **Сакан К.С.**	Соавтор

Автор _____ **Сакан К.С.**

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