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

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

ҚАЙЫРЫМДЫЛЫҚ ҚОРЫ
HALYK
CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»
ЧФ «Халық»

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (350)

APRIL – JUNE 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

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

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

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

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Number 350 (2024). 137–148
https://doi.org/10.32014/2024.2518-1726.272
ӘОЖ (УДК) 004.93’12
ҒТАХР (МРНТИ) 81.93.29

© G. Yesmagambetova[1*], A. Kubigenova[2], A. Aktayeva[3], I. Tseren-Onolt[4], M. Esmaganbet[3], 2024

[1] Sh. Ualikhanov Kokshetau Universuty, Kokshetau, Kazakhstan;
[2] Saken Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan;
[3]A. Myrzakhmetov Kokshetau Universuty, Kokshetau, Kazakhstan;
[4]Mongolian University of Science and Technology, Ulaanbaatar, Mongolia.
E-mail: Gal.esm@mail.ru

METHODS OF BIOMETRIC DATA PROTECTION BASED ON QUANTUM COMPUTING

Yesmagambetova Galiya — Senior Lecturer, Department of Information and Communication Technologies, Sh.Ualikhanov Kokshetau University, Kokshetau, Kazakhstan
E-mail: Gal.esm@mail.ru, https://orcid.org/0000-0002-9868-293X;
Kubigenova Akku — doctoral student, Doctoral student of S.Seifulin Kazakh Agrotechnical Research University, Astana, Kazakhstan
E-mail: akku_kubigenova@mail.ru, https://orcid.org/0000-0002-0342-5253;
Aktayeva Alimbubi — Ph.D., Department of Information Systems and Informatics, A. Myrzakhmetov Kokshetau University, Kokshetau, Kazakhstan
E-mail: aaktaewa@list.ru, https://orcid.org/0000-0002-2693-6785;
Tseren-Onolt Ishdorj — Ph.D., Professor, Department of Computer Science, Mongolian University of Science and Technology, Ulaanbaatar, Mongolia
E-mail: tseren-onolt@must.edu.mn, https://orcid.org/0000-0002-0425-3879;
Esmaganbet Musatai — Ph.D., Professor, Department of Information Systems and Informatics, A. Myrzakhmetov Kokshetau University, Kokshetau, Kazakhstan
E-mail: esmaganbet_m@mail.ru, https://orcid.org/0000-0003-3276-2977.

Abstract. Globalization and informatization of the education system have become a kind of “crash test”: one way or another, educational organizations have had to mobilize all their technical and human resources to preserve the continuity and quality of the educational process. Ensuring security is the biggest problem that has to be faced when implementing proctoring system methods based on multifactor authentication using quantum and post-quantum personality calculations of students in the educational process management system. This paper examines these problems and proposes a new approach to generating a random quantum cryptographic key using the biometric fingerprints of the sender and recipient.

Keywords: biometrics, quantum computing, quantum cryptography, quantum polarization, hash function, quantum one-time password (OTP), two-factor authentication

© Г. Есмагамбетова[1*], А. Кубигенова[2], А. Актаева[3], И. Цэрэн-Онолт[4], М. Есмагамбет[3], 2024

[1]Ш. Уалиханов атындағы Көкшетау университеті, Көкшетау, Қазақстан;
[2]С. Сейфулин атындағы Қазақ агротехникалық зерттеу университеті, Нұр-Сұлтан, Қазақстан;
[3]А. Мырзахметов атындағы Көкшетау университеті, Көкшетау, Қазақстан;
[4]Моңғолия ғылым және технология университеті, Улан-Батор, Моңғолия.
E-mail: Gal.esm@mail.ru

КВАНТТЫҚ ЕСЕПТЕУЛЕРГЕ НЕГІЗДЕЛГЕН БИОМЕТРИЯЛЫҚ ДЕРЕКТЕРДІ ҚОРҒАУ ӘДІСТЕРІ

Есмагамбетова Галия — Ш. Уалиханов атындағы Көкшетау университетінің Ақпараттық-коммуникациялық технологиялар кафедрасының аға оқытушысы, Көкшетау, Қазақстан
E-mail: Gal.esm@mail.ru, https://orcid.org/0000-0002-9868-293X;
Кубигенова Акку — докторант, С. Сейфулин атындағы Қазақ агротехникалық зерттеу университеті, Астана, Қазақстан
E-mail: akku_kubigenova@mail.ru, https://orcid.org/0000-0002-0342-5253;
Актаева Алимбуби — Ph.D., **А**. Мырзахметов атындағы Көкшетау университетінің Ақпараттық жүйелер және информатика кафедрасы, Көкшетау, Қазақстан
E-mail: aaktaewa@list.ru, https://orcid.org/0000-0002-2693-6785;
Цэрэн-Онолт И. — Ph.D., профессор, Информатика кафедрасы, Моңғолия ғылым және технология университеті, Улан-Батор, Моңғолия
E-mail: tseren-onolt@must.edu.mn, https://orcid.org/0000-0002-0425-3879;
Есмаганбет Мусатай — ф.-м.ғ. к., профессор, А. Мырзахметов атындағы Көкшетау университетінің Ақпараттық жүйелер және информатика кафедрасы, Көкшетау, Қазақстан
E-mail: esmaganbet_m@mail.ru, https://orcid.org/0000-0003-3276-2977.

Аннотация. Білім беру жүйесін жаһандандыру және ақпараттандыру “апаттық сынақтың” бір түріне айналды: білім беру ұйымдары білім беру процесінің үздіксіздігі мен сапасын сақтау үшін барлық техникалық және кадрлық ресурстарды жұмылдыруға мәжбүр болды. Қауіпсіздікті қамтамасыз ету — оқу процесін басқару жүйесінде білім Қабылдаушылардың жеке басын кванттық және постквантық есептеулерді пайдалана отырып, көп факторлы аутентификация негізінде прокторинг жүйесінің әдістерін енгізу кезінде кездесетін ең үлкен проблема. Бұл жұмыс осы мәселелерді қарастырады және Жіберуші мен Қабылдаушының биометриялық саусақ іздерін қолдана отырып, кездейсоқ кванттық криптографиялық кілтті құрудың жаңа әдісін ұсынады.

Түйін сөздер: биометрия, кванттық есептеу, кванттық криптография, кванттық поляризация, хэш функциясы, кванттық бір реттік пароль (OTP), екі факторлы аутентификация

© Г. Есмагамбетова[1*], А. Кубигенова[2], А. Актаева[3], И. Цэрэн-Онолт[4], М. Есмагамбет[3], 2024

[1]Кокшетауский университет им. Ш.Уалиханов, Кокшетау, Казахстан;

[2] Казахский агротехнический исследовательский университет им. С.Сейфуллина, Астана, Казахстан;

[3]Кокшетауский университет им А. Мырзахметов, Кокшетау, Казахстан;

[4]Монгольский университет науки и технологии, Улан-Батор, Монголия.

E-mail: Gal.esm@mail.ru

МЕТОДЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ НА ОСНОВЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Есмагамбетова Г. — старший преподаватель кафедры Информационно-коммуникационных технологий, Кокшетауский университет им. Ш.Уалиханова, Кокшетау, Казахстан
E-mail: Gal.esm@mail.ru, https://orcid.org/0000-0002-9868-293X;
Кубигенова А. — докторант, Казахский агротехнический исследовательский университет им. С.Сейфулина, Астана, Казахстан
E-mail: akku_kubigenova@mail.ru, https://orcid.org/0000-0002-0342-5253;
Актаева А. — Ph.D., кафедра Информационных систем и информатики, Кокшетауский университет им. А. Мырзахметов, Кокшетау, Казахстан
E-mail: aaktaewa@list.ru, https://orcid.org/0000-0002-2693-6785;
Цэрэн-Онолт И. — Ph.D., профессор, кафедра Информатики, Монгольский университет науки и технологии, Улан-Батор, Монголия
E-mail: tseren-onolt@must.edu.mn, https://orcid.org/0000-0002-0425-3879;
Есмагамбет М. — к. ф.-м. н., профессор, кафедра Информационных систем и информатики, Кокшетауский университет им. А. Мырзахметов, Кокшетау, Казахстан
E-mail: esmaganbet_m@mail.ru, https://orcid.org/0000-0003-3276-2977.

Аннотация. Глобализация и информатизация системы образования стали своего рода «краш-тестом»: так или иначе образовательным организациям пришлось мобилизовать все свои технические и кадровые ресурсы для сохранения непрерывности и качества образовательного процесса. Обеспечение безопасности — самая большая проблема, с которой приходится сталкиваться при внедрении методов системы прокторинга на основе многофакторной аутентификации с использованием квантовых и постквантовых вычислений личности обучающихся в системе управления учебным процессом. В этой работе рассматриваются эти проблемы и предлагается новый подход к генерации случайного квантового криптографического ключа с использованием биометрических отпечатков пальцев Отправителя и Получателя.

Ключевые слова: биометрия, квантовые вычисления, квантовая криптография, квантовая поляризация, хэш-функция, квантовый одноразовый пароль (OTP), двухфакторная аутентификация

Кіріспе

Жаһандану және ақпараттандыру қоғам жаһандық цифрландырудың арқасында әртүрлі білім беру технологияларын жетілдіруге көптеген мүмкіндіктер жасайды. Білім беру жүйесін жаһандық цифрландыру бұл «апаттық сынақтың» бір түріне айналды: білім беру ұйымдары білім беру процесінің үздіксіздігі мен сапасын сақтау үшін барлық техникалық және кадрлық ресурстарды жұмылдыруға мәжбүр болды. Прокторинг — бұл онлайн-емтихандағы немесе тестілеудегі бақылау процедурасы, онда бүкіл процесті әкімші — проктор бақылайды (ағылш. «proctor» - университеттегі емтихандардың бұзушылықсыз өтуін қамтамасыз ететін адам). Ол емтихан тапсырушының жеке басын анықтайды, оның әрекеттерін веб - камера арқылы бақылайды және компьютер мониторында не болып жатқанын көреді. Бұл технология емтихан алушының жеке басын жоғары ықтималдықпен растауға, оның білімін объективті бағалауға, емтихандағы алдау парақтарын және басқа да амалдарды жоюға мүмкіндік береді. Прокторинг үш негізгі жолмен жүргізіле бастады:

1) проктор-адам-әкімші емтихан барысын веб-камера арқылы бақылайды және бұзушылықтарды қолмен жазады;

2) автопрокторинг-бағдарлама студенттің жеке басын дербес тексереді, оның мінез-құлқын, көзқарасының бағытын бақылайды, бөлмедегі дыбыстарды талдайды, бұзушылықтарды бейнеге тіркейді және есептер дайындайды;

3) адам мен бағдарлама – біріктірілген нұсқа – екі жолмен жүргізілуі мүмкін: а) бүкіл процесс бағдарламаны бақылайды және бұзушылықтар болған жағдайда прокторға сигнал береді; б) әкімші өзі тестіленушілерді онлайн режимінде бақылайды. Соңғы нұсқа ең сенімді болып саналады, өйткені кез-келген бағдарлама сәтсіздікке ұшырауы мүмкін. Сонымен қатар, процесті автоматтандыру арқылы проктор бір уақытта бірнеше студенттен емтихан қабылдай алады және ештеңені назардан тыс қалдырмайды.

Технологияларды ұдайы жетілдіру жағдайында дамудың инновациялық модельдеріне бағдарланған білім беру ұйымдары заманауи технологиялық жаңалықтарды, әсіресе кадрларды даярлаудың жоғары сапасын қамтамасыз етуге, оның ішінде оқыту процесінде қамтамасыз етуге бағытталған жаңалықтарды жедел игеруі қажет. Білім берудегі цифрлық технологиялардың дамуымен прокторинг барған сайын сұранысқа ие болады, осыған байланысты кванттық есептеулер негізінде биометриялық деректерді пайдалана отырып, прокторинг инфрақұрылымының қауіпсіздігін оңтайландыру мүмкіндіктерін зерттеу қажет.

Қауіпсіздікті қамтамасыз ету-оқу процесін басқару жүйесінде білім алушылардың жеке басын кванттық және постквантық есептеулерді пайдалана отырып, көп факторлы аутентификация негізінде прокторинг жүйесінің әдістерін енгізу кезінде кездесетін ең үлкен проблема.

Материалдар мен әдістер

Біздің жұмысымыз негізінен үш ішкі тапсырмадан тұрады: i) биометриялық үлгіні түрлендіру, ii) биометриялық деректерді қауіпсіз тасымалдау, және iii) крипто-биометриялық жүйе.

Ал биометрия - бет, саусақ іздері, көздің торлы қабығы, алақан ізі, сөйлеу және т.б. сияқты мінез-құлық және физиологиялық ерекшеліктері бар адамдардың жеке басының бірегей өлшемі. (Мальтони және т.б., 2003).

Биометриялық жүйеде қолданылатын биометриялық мәліметтер биометриялық сипаттамалар туралы ақпараттың жайлып кетуіне жол бермеуі керек. Сондай-ақ қайтарылмайтын биометриялық деректерді қайтарып алу мүмкіндігін қамтамасыз ету қажет. Құпия сөзге негізделген аутентификация жүйелерінде немесе таңбалауышқа негізделген аутентификация жүйелерінде парольдер немесе таңбалауыштар бұзылған жағдайда оларды өзгерту оңай. Бірақ биометриялық белгілер ажырамас және мәңгілікке бекітіледі, яғни биометриялық деректер қайтымсыз (Мальтони және т.б., 2003).

Биометриялық деректердің иесі олар бұзылған жағдайда биометриялық деректерді қайтарып ала алмайды. Нәтижесінде биометрика мәңгілікке пайдасыз болып қалады (Улудаг және т.б., 2004). Бұл мәселені шешу үшін қайтарылмайтын биометриялық деректерді қайтарып алу мүмкіндігін қамтамасыз ету үшін биометриялық үлгіні (Джейн және т.б., 2013; Рата және т.б., 2007) қайтарылмайтын түрлендіру қажет. Сонымен қатар, бұл биометриялық деректердің құпиялылығын қамтамасыз етеді (Хао және т.б., 2006), сондықтан түрлендірілген үлгі бастапқы үлгі туралы ешқандай ақпаратты жайлып кетпейді. Сонымен қатар, биометриялық деректерді қашықтан пайдалану үшін қорғалмаған байланыс арналары арқылы жіберу керек.

Биометриялық жүйелер құпиялылықты, қауіпсіздікті және биометриялық деректерді қайтарып алу мүмкіндігін қамтамасыз ету үшін биометриялық үлгіні түрлендіруді қажет етеді. Кванттық есептеулерді қолдана отырып, биометриялық деректерді қауіпсіз беру үшін деректерді жасырудың әртүрлі әдістері қолданылады. Саусақ ізі нүктелері кванттық есептеулерді қолдана отырып, беттің немесе синтетикалық саусақ ізінің ішінде жасырылады және қорғалмаған байланыс арнасы арқылы басқа пайдаланушыға жіберіледі. Сол сияқты, саусақ ізі кванттық есептеулерде басқа биометриялық деректерді (мысалы, беттерді) жасыру үшін мұқаба ретінде пайдаланылады және биометриялық деректерді қауіпсіз тасымалдау үшін тасымалдаушы кескін ретінде пайдаланылады. Деректерді жасыру тұжырымдамасында нақты биометрияны мұқаба ретінде пайдалану қауіпті екенін ескеріңіз, өйткені ол Жіберушінің алушыға биометриялық тұлғасын ашады. Кодталған биометрика кездейсоқ мұқабаның дискретті косинус түрлендіруінің (DCT) коэффициент белгісін пайдаланып биттік түрде енгізіледі.

Соңғы уақытта биометрия криптографиямен біріктірілген, гибридті криптобиометриялық жүйе (Хао және т.б., 2006). Демек, кілттерді құру процесіне қатысатын биометриялық деректердің құпиялылығы мен қауіпсіздігіне нұқсан келтірмей, екі түрлі пайдаланушының биометриялық деректері негізінде қайтарылатын және қайтарылмайтын криптографиялық кілтті жасау қажеттілігі туындайды.

Криптографиялық кілттерді шығарумен (Нандакумар және т.б., 2007) немесе криптографиялық кілттерді генерациялаумен (Улудаг және т.б., 2004; Датта және т.б., 2008) байланысты биометрияны криптографиямен біріктіру көптеген аспектілерде перспективті болып табылады.

Биометрия иесімен тікелей байланысты болғандықтан, бұл криптографиялық кілтті есте сақтау мәселесін жояды және пайдаланушылардың бас тартпайтындығын растайды. Алайда, криптобиометриялық жүйенің кейбір проблемалары бар. Кез келген биометриялық жүйе биометриялық деректердің құпиялылығы мен қауіпсіздігін растайтын биометриялық үлгілерді қорғауды қамтамасыз етуі керек

(Джейн және т.б., 2013).

Бұлыңғыр кванттық есептеулерге ***негізделген қауіпсіздікті талдау***. Бұл бөлімде қауіпсіздіктің екі аспектісі қарастырылады және талданады: бір жағынан, жасырындық пен байланысты қанағаттандыру үшін анық емес кванттық есептеу талданады; екінші жағынан, бір реттік кванттық кілттерге (OTP) негізделген биометриялық аутентификацияның қауіпсіздігі талданады.

Кванттық бұлыңғыр уәделердің қауіпсіздігі. Біріншіден, біз жасырындықты талдаймыз. Қабылдаушы беретін міндеттеме фазасында міндеттемелерді ұсынады $Q_{Hв}(|k_j\rangle),\Delta_в$, онда $\Delta_в$ және мәні хэш-функциялар $Q_{Hв}(|k_j\rangle)$, екеуі де тиісінше қамтитын бөлігі ақпарат $Q_{Hв}(|k_j\rangle)$, ал әділетсіз Жіберуші алушы фазаны ашқанға дейін міндеттеме туралы ақпарат алу үмітімен алдауға тырысады $|k_j\rangle$.

Ол туралы ақпарат алады, комминттере екі тәсілмен: (1) бір амалын тап болжамды мәні $|\varphi_j\rangle_L$ негізінде $\Delta_в(|k_j\rangle)$ және кодсыздандыру оны алу үшін $|k_j\rangle$ (2) искать мәні соқтығысу хэш-функциялар $Q_{Hв}(|k_j\rangle)$, және іздеу мәні соқтығысу қанағаттандыратын талабы

$$Q_{Hв}(|k_j\rangle) = Q_{Hв}(|\tilde{k}_j\rangle) \quad (1)$$

Біріншіден, бірінші жағдай талданады: өйткені код құрылымы туралы ақпараттың бір бөлігін қамтиды $|\varphi_j\rangle_L$ Жіберуші кванттық кодты декодтау әдісін қолдана отырып, міндеттемелер туралы ақпарат алуға тырысады. $\Delta_в$ - бұл n кванттық биттермен бірдей жасырын сөз $|\varphi_j\rangle_L$, және оның жалпы саны ше $|1\rangle$ t қателерді түзету мүмкіндіктерді арттырады.

Егер Жіберуші кодты осыған сәйкес декодтайтын болса, онда дұрыс код сөзін $|\varphi_j\rangle_L$ алу мүмкін емес, өйткені ол кванттық кодтың қателерді түзету мүмкіндіктерінен асып түседі. Аутентификация жүйесі қателерді түзетудің кванттық кодтары процесіне ұқсас процесте $\Delta_в = D_в(|\phi\rangle), |\varphi_j\rangle_L$ есептейді. Бұл процесс кванттық қателерді түзету коды ұшыраған қате операторының әрекетіне ұқсас және нәтиже болып табылады. Ішкі кеңістіктерге бейнелеу кезінде сөздің жалпы мағынасында оңтайлы декодтау бар, яғни қателерді түзетумен субдекодтау стратегиясына сәйкес ең ықтимал қатені іздеу,қате код сөзінің ең жақын заңды код сөзін іздеу, яғни максималды ықтималдылық принципі бойынша кванттық декодтау. декодтау.

Максималды ықтималдылықтың таңдалмаған кванттық декодтауының және максималды ықтималдылықтың қарапайым кванттық декодтауының егжей-тегжейлі дәлелі әдебиетте келтірілген (Улудаг және т.б., 2004; Янг & Вербаухеде, 2005).

Максималды ықтималдылықты декодтау және жеңілдетілген кванттық декодтау бірдей NP есептері болып табылады және мұндай есептерді Фурье үлгісін кванттық талдау жағдайында да тиімді шешу мүмкін емес, яғни кванттық кодты Фурье үлгісін кванттық талдау жағдайында да тиімді шешу мүмкін емес дегенді білдіреді, яғни бұл кванттық машиналар Тьюринг алгоритмге алгоритмдік шабуылды тиімді орындай алмайды.

Осылайша, алушы анық емес дәлел келтірмейінше, яғни аутопсия кезеңіне дейін Жіберуші ақпаратты сәтті бұрмалай алмайды. Әрі қарай, біз шабуылдың екінші сценарийін талдаймыз хэш-функциясының соқтығысу мәнін іздеу $Q_{Hв}(|k_j\rangle)$. Реті кванттық бит, кездейсоқ таңдалған пайдаланушы тіркеу кезеңінде $|k_j\rangle$ бірі болып табылады 2^k - өлшемді гильбертттік шарттары кеңістікте және Жіберуші $Q_{Hв}(|k_j\rangle)$ хэш-мәнін хэш-функциясын іздейді, бұл баламалы іздеу хэш- мәні $Q_{Hв}(|k_j\rangle)$, және күрделі іздеу тікелей байланысты маңызы бар айнымалы k, ол әдетте қолайлы таңдалады.

Жалпы алғанда, сәйкес k мәні және келесі байланыстыру талдауында қарастырылатын және биометриялық аутентификация қауіпсіздігін талдаудағы кванттық хэш алгоритмі процесімен біріктірілетін қажетті қауіпсіздік талаптарына қол жеткізу үшін кванттық реттілікпен құрылған 2^k өлшемді Гильберт кеңістігі жеткілікті үлкен болатындай етіп таңдалады.

Байланысты сапалық талдау, фазасындағы ашу міндеттемелерді, егер әділетсіз Қабылдаушы алдауды күтсе, басқа сөзбен айтқанда, фаза ашылу кезеңі Жіберушіге бастапқы міндеттемеден өзгеше нәрсені білдіреді алдауды күтеді, яғни ашылу кезеңінде Жіберушіге басқа бит ұсынады, содан кейін алушы хэш-соқтығысуларын іздеуі керек, яғни $Q_{Hв}(|k_j\rangle)$ хэш мәнімен сәйкес келетін хэш мәні бар соқтығысулар $Q_{Hв}(|k_j\rangle)$ (, бірақ $\varphi_j\rangle_L$ кодтық сөзден (сәйкес кодты сөз $|k_j\rangle$) ерекшеленеді. Ең бастысы, соқтығысу-дәлелдеу жұбын құру қажет $(\Delta_в'',\Delta_в''')$ мұндағы $\Delta_в''$ - адал міндеттеменің дәлелі, ал $\Delta_в'''$ - сәтті алдануы мүмкін міндеттеменің дәлелі, бірақ $D_в(\Delta_в',\Delta_в'')$ және $D_в(\Delta_в',\Delta_в''')$ әр түрлі жерлерде кездеседі, бұл бір-бірінің орнына міндеттемелердің бұлыңғыр дәлелі ретінде пайдаланылмайтындығының дәлелі ретінде қарастырылады, өйткені болжам бойынша, бұл бір-бірімен алмастырылуы мүмкін, ал алаяқтық міндеттеменің дәлелі, өз кезегінде, алаяқтық міндеттеменің кодтық сөзін алу үшін декодтауды қамтамасыз ете алады $|\varphi_j\rangle_L$, сонымен бірге ол декодталады, содан кейін хэштеледі. Декодтау мен хэштеуден кейін алынған нәтиже $Q_{Hв}(|k_j\rangle)$, бұл шартты орындау мүмкін емес. Бұл шартты орындау мүмкін емес. Осылайша, бұл әдіс алушының сәтті қолдан жасалмауын қамтамасыз етеді, яғни хаттама міндетті болып табылады.

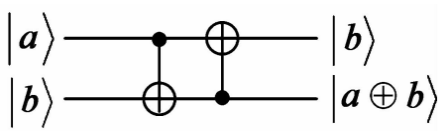
Биометриялық аутентификация қауіпсіздігі. Кванттық бұлыңғыр уәделердің қауіпсіздігімен салыстырғанда, кванттық бұлыңғыр уәделерге негізделген қоңырау және жауап биоаутентификациясының қауіпсіздігі басқа фокусқа ие.

Бірінші жағдайда, басты назар Жіберуші мен міндеттемелерді алушы арасындағы жасырындық пен байланыстың қауіпсіздігіне, ал екіншісінде келушінің тіркеу ақпаратын сақтау (немесе беру) қауіпсіздігіне және келушінің аутентификациясын алу кезінде аутентификация жүйесінің қауіпсіздігіне аударылады, осылайша шабуылдаушы өзін заңды пайдаланушы ретінде көрсетпейді және ауыстыру арқылы жүйеге басып кірмейді.

Біріншіден, біз тіркеу ақпаратын сақтау қауіпсіздігін талдаймыз. Пайдаланушыны тіркеу кезеңінде жүйе хэш мәнін жасайды $Q_{Hв}(|k_j\rangle)$ және жалпыланған белгісіз қашықтық , және оларды орталық дерекқорда сақтайды, сондықтан шабуылдаушы, $\{Q_{Hв}(|k_j\rangle)\Delta_в\}$, деректерін алса да, олардан кез келген

сенімді ақпаратты шеше алмайды

$Q_{Hв}(|k_j\rangle)$ деректерінің қауіпсіздігіне келетін болсақ, оны кванттық хэш алгоритмі тұрғысынан талқылайық: классикалық хэш алгоритмі сияқты, негізгі талап бір бағытты функцияның қасиеті болып табылады. Кванттық есептеу ортасында кванттық өлшемдер кванттық күйдің күйреуіне әкелуі мүмкін және бұл қайтымсыз процесс, алайда ол кванттық хэш функциясын құруға жарамайды. Кванттық өлшемдер көбінесе проекция үшін кванттық биттерге ортогональды болғандықтан, пайда болатын коллапс сөзсіз кванттық ақпараттың жоғалуына әкеледі және бұл ақпараттың жоғалуын болжау мүмкін емес, әртүрлі бастапқы кванттық күйлердің үлкен саны болады, бір соңғы күйге құлағаннан кейін, бұл біз көргіміз келмейтін хэш соқтығысуы деп аталады. Сондықтан, классикалық хэш алгоритмдерін құру сияқты $H: \{0,1\}^n \to \{0,1\}^m$, картаға түсіру қатынасын құруға негізделген симметриялы криптографиялық алгоритмдердің үлкен класы бар, сондықтан n = m (жалпы жағдайда қысу дисплейі, яғни n > m)), соқтығысуды болдырмау үшін мүмкіндігінше болдырмауға болады. Біз кванттық хэш алгоритмін келесідей құрамыз және оны хэш мәндерін сақтау қауіпсіздігін талдау үшін қолданамыз: 1-суретте көрсетілгендей құрамыз (Semi-Swap).



Сурет 1 - Кванттық хэш алгоритм

Мұндағы i = 1,2, …, ⌊k/2⌋, |a⟩, |b⟩ ∈ {|0⟩, |1⟩} $G[\cdot]$ қолданып түрлендіру жасайды, оның реттілігі кванттық бит $|k_j\rangle$ орындау үшін обфускации және диффузия алу үшін жаңа дәйектілігі k кванттық бит $G[|k_j\rangle] = |k_j\rangle^{\otimes k}$; содан кейін келесі $\{P_{uv}\} = \{I_{00}, X_{01}, Y_{10}, Z_{11}\}$ операторларының жинағын жасайды, мұнда жолма-жол индексі uv∈ GF(22), I - оператор баламалылығын, ал X, Y және Z - Паули операторлары. Содан кейін келесі операторлар жиынтығын жасаңыз. GF(22) кеңейтілген аймағына кезекпен $|k_j\rangle$ тізбегін көрсететін кезектілік кілт ретінде пайдаланылады және сәйкес оператор $\{P_{uv}\}$ операторлар жиынтығынан кілтке сәйкес таңдалады және түрлендіруі $G[|k_j\rangle]$ қолданылады:

$$\mathfrak{E}\{\xi, G[|k_j\rangle]\} = (P_{uv}\{|k_j\rangle\})^{\otimes k} \qquad (2)$$

Өзгеретін жоғарыда аталған барлық процестер түрлендіру, яғни алу үшін кванттық хэш-мәндері $Q_{Hв}(|k_j\rangle) = P_{uv}\{(|k_j\rangle)\}^{\otimes k}$. Бүкіл процесс хэштеу - бұл ең алдымен, жүйелілігі $k_j\rangle$ жүзеге асырған үшін обфускации диффузия, содан кейін реті $k_j\rangle$ анықтау үшін пайдаланылады кілтті таңдау үшін $\{P_{uv}\}$, тиісінше, бит операторын жою үшін $|k_j\rangle^{\otimes k}$.тең ұзындықтағы шифрлауға қол жеткізеді. Кілт пайдаланылады ең реттілігін $|k_j\rangle$ үшін зиянкес, тіпті егер алгоритмі жария шарт болып табылады, бірақ кілті жоқ белгілі ретпен $|k_j\rangle$ шешім, жүйелілігі $|k_j\rangle$ кездейсоқ құрастырып, әр кезеңде тіркеу, процес қауіпсіздігін шифрлау ұқсас

клалассикалық ортада бір рет құпия пароль сондықтан соңғы хэш-мәні сақтау қауіпсіз.

Енді біз жалпыланған анық емес қашықтықтың деректерінің қауіпсіздігін талдаймыз. $\Delta_в$, тіркеу кезеңінде аутентификация жүйесі есептейді $\Delta_в = D_в(|\phi\rangle, |\varphi_j\rangle_L)$, саусақ ізі үлгісінің әсері $|\phi\rangle$ арна қатесінің векторы ретінде қарастырылуы мүмкін (шу), код сөзінің рөлі, $|\varphi_j\rangle_L$, Шу арқылы код сөзіне тең болатын жалпыланған, анық емес қашықтықтың $\Delta_в$ нәтижесі.

Шу арнасынан кейінгі код сөзіне тең болатын жалпыланған, анық емес қашықтықтың $\Delta_в$ нәтижесі. Өйткені салмағы үлгідегі саусақ іздерін $|\phi\rangle$ артық қабілеті қателерді түзету t коды $|k_j\rangle$ арналған $|\varphi_j\rangle_L$, егер шабуылдаушы дұрыс декодтай алмаса $|k_j\rangle$, декодтау алгоритмі жалпыға қол жетімді болады. Бұл қауіпсіздік жоғарыда аталған кванттық қателерді түзету кодын декодтаудың NP тапсырмасына негізделген, ол мұнда қайталанбайды.

Әрі қарай, біз аутентификация процесінде заңды пайдаланушылар ретінде көрінетін және алдау арқылы жүйеге енетін зиянкестердің мәселесін талдаймыз. Бұл қауіпсіздік проблемасы жоғарыда талқыланған $\Delta_в$ деректер қауіпсіздігінің мәселесін талдаумен тығыз байланысты: заңды пайдаланушы аутентификация үшін саусақ ізінің үлгілерін ұсынады $|\phi'\rangle$, олар тіркеу кезінде үлгілермен бір деректемелерден алынуы керек, бірақ шамалы айырмашылықтарға ие болуы мүмкін (бұл анық емес міндеттеменің мәні), ал аутентификация сатысындағы жүйе есептейді. $\Delta_в = D_в(\Delta_в, |\phi'\rangle$, өйткені $|\phi\rangle$ және $|\phi'\rangle$ бір заңды пайдаланушының саусақ іздерінің үлгілері болып табылады, шамалы айырмашылықтарға ие, бірақ бұлыңғыр шекті шектерде, Δ′ е, жүйемен есептелген, код сөзіне баламалы, $|\varphi_j\rangle_L\rangle$, онда t биттері аз қате операторының әсеріне ұшырайды, сондықтан оны алу үшін дұрыс декодтауға болады $|k_j\rangle$.

Алайда, егер шабуылдаушы аутентификация үшін саусақ іздерінің үлгілерін ұсынса $|\varphi''\rangle$ және $|\phi\rangle$, олар міндетті түрде бір-бірінен ерекшеленеді және белгісіз шекті деңгейден асады (бұл анық емес міндеттеменің мәні), жүйе орындайды $\Delta''_в = D_в(\Delta_в, |\phi''\rangle)$, содан кейін оларды декодтайды және қате тізбектердің салмағы, $\Delta''_в$ әсер ететін қате тізбектің салмағы t-ден үлкен болғандықтан, оны алу үшін сәтті декодтау мүмкін емес. $|k_j\rangle$, ал шабуылдаушы шабуылды сәтті жүзеге асыра алмайды.

Қорытынды

Криптографиялық кілтті құру және оған қызмет көрсету дәстүрлі криптографияның екі маңызды мәселесі болып табылады. Криптографиялық кілт оны болжау қиын болатындай етіп жасалуы керек, содан кейін оны пайдаланушылардың үстеме шығындарынсыз басқару керек.

Бұл жұмыс осы мәселелерді қарастырады және Жіберуші мен алушының биометриялық саусақ іздерін қолдана отырып, кездейсоқ кванттық криптографиялық кілтті құрудың жаңа әдісін ұсынады.

Біздің жұмысымызда саусақ ізі деректерінің құпиялылығы мен қауіпсіздігі шаблон арқылы қамтамасыз етіледі. Сонымен қатар, біз кілтті қайтарып алуға болатын хаттаманы ұсынамыз, бұл биометриялық белгінің қайтарылмайтын қасиетінің шектелуін жояды. Ең бастысы, кілтті байланысқа дейін сақтаудың

қажеті жоқ.

Шындығында, хаттама әртүрлі сеанстарда әртүрлі кілттерді жасауға мүмкіндік беру арқылы қауіпсіздікті арттырады. Ұсынылған криптобиометриялық жүйе көптеген шабуылдарға төзімді, мысалы, белгілі кілт шабуылдары, қайта ойнату шабуылы, ортадағы адам шабуылдары және т.б. Прокторинг студенттердің оқу жетістіктерін диагностикалау нәтижелерінің сенімділігі мен сенімділігін арттыруға мүмкіндік береді. Прокторлар, аудиториядағы емтихан үйлестірушілері сияқты, қатысушылар онлайн емтихандарды тапсыру кезінде ережелерді сақтауы үшін процесті бақылайды (тапсырмаларды өз бетінше орындайды және сыртқы материалдар мен қосымша ресурстарды пайдаланбайды). Осылайша, біз ұсынған тәсіл тиімді шешімдерді ұсынады, онда біз хабарламаны қорғалмаған желілік арна арқылы жіберу кезінде сеанстық криптографиялық кілт қажет.

ӘДЕБИЕТТЕР

Алдын ала шифрлау стандартты Aes (AES). (2001). Федералдық ақпаратты өңдеу стандарттарының басылымы 197. Америка құрама штаттарының Ұлттық стандарттар және технологиялар институты (NIST). — https://doi.org/10.6028/NIST.FIPS.197

Бодо А. (1994). Биометриялық ерекшелігі бар цифрлық қолтаңбаны алу әдісі. — Неміс патенті DE 4243908A1

Болле Дж., Коннелл С., Панканти Н., Рата А. (2003). Биометрия бойынша аға гид. — Спрингер-Верлаг, Нью-Йорк.

Гаддам С., Лал М. (2010). Криптография үшін тиімді жойылатын биометриялық кілттерді генерациялау схемасы. Int. J. — Netw. Secur. —11(2). — 57-65.

Датта С., Кар А., Чаттерджи Б. (2008). Биометриялық және криптографияны қолданатын желілік қауіпсіздік. Springer Berlin Heidelberg. Солтүстік Каролина. Маханти, Proc. Adv. Intell тұжырымдамалары. қарсы.сист. — LNCS 5259. — 38–44 бб.

Джагадисан А., Дурайсвами К. (2010). Мультимодальды биометрикадан криптографиялық кілттерді генерациялауды қамтамасыз етті: саусақ ізі мен иристің мүмкіндік деңгейіндегі синтезі. Int. J. Comput. Sci. Inform. Secur. — 7(2). — 28–3. — https://doi.org/10.48550/arXiv.1003.1458

Джагадисан А., Тиллайккараси Т., Дурайсвами К. (2010). Бірнеше биометриялық әдістерден криптографиялық кілттерді жасау: ұсақ бөлшектерді ирис функциясымен біріктіру. Int. J. Comput. Sci. Inform. — Secur 2(6). — 1–26 бб.

Джейн А., Нандакумар К., Нагар А. (2013). Биометрикадағы қауіпсіздік және құпиялылық саласында. Саусақ ізі үлгісін қорғау: теориядан практикаға дейін. Springer London, 187-214 б. - DOI:10.1007/978-1-4471-5230-9_8

Канаде С., Камара Д., Кричен Э., Петровска-Делакретаз Д., Дорицци Б. (2008). Ирис көмегімен биометриялық негіздегі криптографиялық кілттерді қалпына келтірудің үш факторлы схемасы. 6--шы биометрия симпозиумының материалдарында (BSYM). — Тампа, Флорида. — АҚШ. — 59–64 бб.

Канаде С., Петровска-Делакретаз Д., Дорицци Б. (2010). Қауіпсіз криптографиялық қосымшалар үшін биометрикаға негізделген сеанс кілттерін құру және бөлісу. Биометрия бойынша IEEE төртінші халықаралық конференциясының материалдарында: теорияның қолданылуы мен жүйелері (BTAS). — Вашингтон, Колумбия округі. — 1–7 бб.

Клейн Д.В.. (1990). Крекерді Бұзады: 2-ШІ USENIX Қауіпсіздік шеберханасының (Портленд) материалдарындағы пароль қауіпсіздігін зерттеу және жақсарту. Крекерді бұзу: пароль қауіпсіздігін зерттеу және жақсарту. — 5–14 бб. — https://doi.org/10.1.1.11.6491&rep=rep1&type=pdf

Мальтони Д., Майо Д., Джейн А., Прабхакардың С. (2003). Саусақ іздерін тану жөніндегі анықтамалығы. — Спрингер-Верлаг, Нью-Йорк. — DOI:10.1007/b97303

Митник К., Саймон В., Возняк С. (2002). Алдау өнері: Адам қауіпсіздігінің элементін басқару. — Уайли, Нью-Йорк

Монроуз Ф., Рейтер М.К., Ли К., Ветцель С. (2001). IEEE Қауіпсіздік және құпиялылық симпозиумының материалдарында. дауыстан криптографиялық кілттерді генерациялау. IEEE Computer Society Washington. — DC USA. — 202–213 б.

Нандакумар К., Джейн А., Панканти С. (2007). Саусақ ізіне негізделген бұлыңғыр қойма: Енгізу

және орындау.. IEEE Trans. Inf. Forensics Secur. 2(4), 744-757.

Рата Н., Чиккерур С., Коннелл ДЖ.Х., Болле R.M. (2007). Жойылатын саусақ ізі үлгілерін жасайды. IEEE Trans. Pattern Anal. — Mach. Intell. — 29(4). —561–572.

Рата Н.К., Коннелл Д.Ж., Болле Р. (2001). Биометриялық Аутентификация жүйесіндегі қауіпсіздік пен құпиялылықты жақсарту. — IBM жүйесі. Дж. — 40(3). — 614–634.

Росс А., Джаин А. (2003). Биометрикадағы ақпараттық синтезі. Үлгіні тану. —Lett. 24. —2115–2125.

Сталлингс В. (2010). Криптография және Желілік Қауіпсіздік: Принциптері мен Практикасы. – Прентис Холл.

Улудаг У., Панканти С., Прабхакар С., Джейн А. (2004). Биометриялық криптожүйелері: Мәселелері мен қиындықтары. Proc. — IEEE. — 92(6). — 948–960.

Фэн Х., СС. (2002). Онлайн қолжазба қолтаңбаларынан Wah Жеке кілт генерациясы. Inform Manag. Comput. Secur. —10(4). — 159–164.

Хао Ф., Андерсон Р., Даугман Дж. (2006). Криптографияны биометрикамен тиімді үйлестіреді. IEEE Trans. Comput — 55(9). — 1081–1088.

Чарльз Н., Кияваш Д. (2003). ACM SIGMM биометрия әдістері мен қолдану бойынша семинарының материалдарында. Lin, smartcard негізіндегі саусақ ізінің қауіпсіз аутентификациясы. — ACM Нью-Йорк, АҚШ. — 45–52 бб. — https://doi.org/10.1145/982507.982516

Чен Б., Чандран В. (2007). Сандық кескінді есептеу әдістері мен қолданбалары бойынша австралиялық үлгіні тану қоғамының. 9-шы екіжылдық конференциясының материалдарында. беттерден биометриялық негіздегі криптографиялық кілттерді генерациялау. — Glenelg Australia. — 394–401 б.

Янг С., Вербаухеде И. (2005). Сот процесінде (ICASSP›05) акустика, сөйлеу сигналдарды өңдеу бойынша IEEE Халықаралық конференциясы. — Том. 5. Бұлыңғыр қойма схемасына негізделген саусақ іздерін автоматты түрде қауіпсіз тексеру жүйесі. IEEE Philadelphia, Pennsylvania. — USA. — Pp. в/609–в/612.

REFERENCES

Advance Encryption Standard AES. (2001). Federal Information Processing Standards Publication 197. (United States National Institute of Standards and Technology (NIST). — https://doi.org/10.6028/NIST.FIPS.197

Bodo A. (1994). Method for Producing a Digital Signature with Aid of Biometric Feature. — German Patent DE 4243908A1.

Bolle J.H. R.M., Connell S., Pankanti N.K., Ratha A.W. (2003). Senior Guide to Biometrics. (Springer-Verlag. — New York. — https://doi.org/10.1007/978-1-4757-4036-3

Charles N.C.T., Kiyavash D.J. (2003). in Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications. Lin, Secure smartcard based fingerprint authentication. — ACM New York, NY, USA. — Pp. 45–52. — https://doi.org/10.1145/982507.982516

Chen B., Chandran V. (2007). in Proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications. Biometric Based Cryptographic Key Generation from Faces (Glenelg Australia. — Pp. 394–401. — DOI:10.1109/DICTA.2007.4426824

Dutta S., Kar A., Chatterji B.N., Mahanti N.C. (2008). in Proc. Adv. Concepts Intell. Vis.Syst. — LNCS 5259. — Network Security Biometric And Cryptography (Springer Berlin Heidelberg. —*P*p. 38–44. — DOI:10.1007/978-3-540-88458-3_4

Feng H., Wah C.C. (2002). Private key generation from on-line handwritten signatures. Inform Manag. Comput. Secur. — 10(4). —159–164. — DOI:10.1108/09685220210436949

Gaddam SVK., Lal M. (2010). Efficient Cancellable Biometric Key Generation Scheme for Cryptography. Int. J. Netw. Secur. 11(2), 57-65.

Hao F., Anderson R., Daugman J. (2006). Combining Crypto with Biometrics Effectively. IEEE Trans. Comput. 55(9), 1081-1088. - **DOI:** 10.1109/TC.2006.138

Jagadeesan A., Duraiswamy K. (2010). Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. Int. J. Comput. Sci. Inform. Secur. — 7(2). — 28–37. — https://doi.org/10.48550/arXiv.1003.1458

Jagadeesan A., Thillaikkarasi T., Duraiswamy K. (2010). Cryptographic Key Generation from Multiple Biometrics Modalities: Fusing Minutiae with Iris Feature. Int. J. Comput. Appl. — 2(6). — 16–26.

Jain A.K., Nandakumar K., Nagar A. (2013). in Security and privacy in biometrics. Fingerprint Template Protection: From Theory to Practice (Springer London. — Pp. 187–214. — DOI:10.1007/978-1-4471-5230-9_8

Kanade S., Camara D., Krichen E., Petrovska-Delacretaz D., Dorizzi B. (2008) in Proceedings of 6th Biometrics Symposium (BSYM 2008). Three Factor Scheme for Biometric-Based Cryptographic Key Regeneration Using Iris. Tampa, Florida. — USA. — Pp. 59–64. — DOI:10.1109/BSYM.2008.4655523

Kanade S., Petrovska-Delacretaz D., Dorizzi B. (2010). in ˜ Proceedings of Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington. — DC, USA, 2010. Generating and sharing biometrics based session keys for secure cryptographic applications. — Pp. 1–7. — DOI:10.1109/BTAS.2010.5634545

Klein D.V. (1990). Foiling the Cracker": A Survey of, and Improvements to, Password Security, in Proceedings of the 2nd USENIX Security Workshop (Portland). — Foiling the cracker: A survey of, and improvements to, password security. —*P*p. 5–14. — https://doi.org/10.1.1.11.6491&rep=rep1&type=pdf

Maltoni D., Maio D., Jain A.K., Prabhakar S. (2003). Handbook of Fingerprint Recognition. Springer. — Verlag, New York. — DOI:10.1007/b97303

Mitnick K., Simon W., Wozniak S. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley, New York, - ISBN: 978-0-471-23712-9

Monrose F., Reiter M.K., Li Q., Wetzel S. (2001) in Proceedings of IEEE Symposium on Security and Privacy. Cryptographic key generation from voice. — IEEE Computer Society Washington. — DC USA. — *P*p. 202–213. — DOI:10.1109/SECPRI.2001.924299

Nandakumar K., Jain A., Pankanti S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. — IEEE Trans. Inf. Forensics Secur. — **2**(4). —744–757. — DOI:10.1109/TIFS.2007.908165

Ratha N.K, Connell J.H, Bolle R. (2001). Enhancing Security and Privacy in Biometric-Based Authentication System. — IBM Syst. J. — 40(3). — 614–634. — DOI:10.1147/sj.403.0614

Ratha N.K., Chikkerur S., Connell J.H., Bolle R.M. (2007). Generating Cancellable Fingerprint Templates. — IEEE Trans. Pattern Anal. Mach. Intell. —29(4). — 561–572. — DOI:10.1109/TPAMI.2007.1004

Ross A., Jain A.K. (2003). Information fusion in biometrics. Pattern Recognit. — Lett. 24. — 2115–2125. — DOI:10.1007/3-540-45344-X_52

Stallings W. (2010). Cryptography and Network Security: Principles and Practice. — Prentice Hall. — ISBN 13: 978-0-13-609704-4

Uludag U., Pankanti S., Prabhakar S., Jain A.K. (2004). Biometric Cryptosystems: Issues and Challenges. Proc. IEEE. — 92(6). — 948–960. — **DOI:** 10.1109/JPROC.2004.827372

Yang S., Verbauwhede I. (2005). in Proceedings (ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing. — Vol. 5. Automatic secure fingerprint verification system based on fuzzy vault scheme. — IEEE Philadelphia, Pennsylvania, USA. — Pp. v/609–v/612. — DOI: 10.1109/ICASSP.2005.1416377

МАЗМҰНЫ

Н. Абдразакұлы, Л. Черикбаева, Н. Мукажанов, Ж. Алибиева

АНСАМБЛЬДІК ТӘСІЛ НЕГІЗІНДЕ КЕСКІНДІ ӨҢДЕУДІҢ ТИІМДІ АЛГОРИТМІН ҚҰРУ.....7

Б.Т Абыканова, А.А. Таутенбаева, А.Г. Амангосова, Г.Т. Бекова, А.Ж. Акматбекова

ӨЗДІГІНЕН БІЛІМ АЛУШЫЛАРДЫ ЖЕТІЛДІРУ МЕН ДАМЫТУДАҒЫ ИНТЕРАКТИВТІ БІЛІМ БЕРУ ТЕХНОЛОГИЯЛАРЫ.....30

Ж.Ж. Ажибекова, Д.И. Усипбекова, Б.Н. Джаханова, К. Жыланбаева, Ә.Н. Тұрсун

МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІМЕН ҒАРЫШТЫҚ ҚЕСКІНДЕРДЕН БҰЛТТАР МЕН ТҰМАНДЫҚТАРДЫ ЖОЮ.....43

М. Айтимов, Г.Б. Абдикеримова, К.К. Макулов, Б.А. Досжанов, Р.У. Альменаева

МАШИНАЛЫҚ ЖӘНЕ ТЕРЕҢ ОҚЫТУ АЛГОРИТМДЕРІ АРҚЫЛЫ МӘТІННІҢ ЭМОЦИОНАЛДЫҚ ЖАҒДАЙЫН ЗЕРТТЕУ.....57

А.Т. Акынбекова, А.А. Муханова, Salah Al-Majeed, Г.С. Алтаева

АЙМАҚТЫ ДАМЫТУДЫҢ ӘЛЕУМЕТТІК ПРОЦЕСТЕРІН БАҒАЛАУ ҮШІН ШЕШІМДЕР ҚАБЫЛДАУДЫҢ БҰЛДЫР МОДЕЛЬДЕРІ.....69

К.М. Алдабергенова, А.Б. Касекеева, М.Ж. Айтимов, К.К. Дауренбеков, Т.Н. Есикова

АГРОӨНЕРКӘСІП КЕШЕНІНІҢ ЛОГИСТИКАСЫНЫҢ МАРКЕТИНГТІК БАСҚАРУЫН ЖЕТІЛДІРУ.....85

А.Е. Әбжанова, А.А. Быков, С.К. Сагнаева, Е.Ә. Әбжанов, Д.И. Суржик

ЖЕР АСТЫ ЖЕР АСТЫ СУЛАРЫН ЕСКЕРЕ ОТЫРЫП, ТОПЫРАҚТЫ МОДЕЛЬДЕУДІ ОҢТАЙЛАНДЫРУ.....96

А.М. Бисенгалиева, А.У. Исембаева, Т.К. Душаева, Н.М. Алмабаева, Г.О. Ильясова

СЕМАНТИКАЛЫҚ ДЕРЕКТЕРДІ ТАЛДАУ АРҚЫЛЫ КІЛТ СӨЗДЕРДІ ҚАМТУ.....108

А.Х. Давлетова, Н.Н. Оразова, Ж.Б. Сайлау, Д.Н. Курмангалиева, Г.Л. Абдугалимов

БАСТАУЫШ СЫНЫП ОҚУШЫЛАРЫН ХАЛЫҚАРАЛЫҚ PIRLS ЗЕРТТЕУІНЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР АРҚЫЛЫ ДАЯРЛАУ ЖОЛДАРЫ.....120

Г. Есмагамбетова, А. Кубигенова, А. Актаева, И. Цэрэн-Онолт, М. Есмагамбет

КВАНТТЫҚ ЕСЕПТЕУЛЕРГЕ НЕГІЗДЕЛГЕН БИОМЕТРИЯЛЫҚ ДЕРЕКТЕРДІ ҚОРҒАУ ӘДІСТЕРІ.....137

Г.Қ. Ешмұрат, Л.С. Каинбаева,

МАТЕМАТИКАЛЫҚ ҮРЕЙ ЖӘНЕ ОНЫҢ БОЛАШАҚ МАТЕМАТИКА ПӘНІ МҰҒАЛІМДЕРІНІҢ МАНСАБЫНА ӘСЕРІ.....149

Т.К. Жукабаева, В.А. Десницкий, Е.М. Марденов

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕРДЕГІ ДЕРЕКТЕРДІ ЖИНАУ, ӨҢДЕУ ЖӘНЕ ТАЛДАУ ӘДІСТ ЕМЕСІ.....163

А.М. Джумагалиева, А.Ә. Шекербек, Ж.Ж. Хамитова, М. Свобода, С.А. Қалдар

АДАПТИВТІ АНОМАЛИЯНЫ АНЫҚТАУ ЖҮЙЕЛЕРІНІҢ КИБЕРҚАУІПСІЗДІГІН МАШИНАЛЫҚ ОҚЫТУ АРҚЫЛЫ АРТТЫРУ.....177

А.А. Исмаилова, Г.Е. Мырзабекова, М.Ж. Базарова, Г.Ж. Нурова, Г.Т. Азиева

ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІН ПАЙДАЛАНУ АРҚЫЛЫ ҚАРЖЫ НАРЫҒЫНДАҒЫ БАҒАЛАРДЫ БОЛЖАУ.....190

К. Кощанова, Сапарбайқызы, К.Е. Жангазакова, А.С. Сағынбай, Э. Куриэль-Марин

STEM-ДЕ БІЛІМ БЕРУ ӘЛЕУЕТІН БАРЫНША ПАЙДАЛАНУ: ОҚУ НӘТИЖЕЛЕРІН ЖАҚСАРТУҒА ҮЛЕС, ҚИЫНДЫҚТАР ЖӘНЕ СТРАТЕГИЯЛАР.....205

А.А. Мұханова, С.К. Кожукаева, Л.Г. Рзаева, Ж.Е. Доумчариева, У.Т. Махажанова

МЕДИЦИНАЛЫҚ БЕЙНЕЛЕР НЕГІЗІНДЕ КӨЗ ТОРЫНЫҢ АУРУЛАРЫН ДИАГНОСТИКАЛАУ ҮШІН ТЕРЕҢ ОҚЫТУ МОДЕЛЬДЕРІН ҚОЛДАНУ ЖӘНЕ ТАЛДАУ..218

Ә.Ж. Омуртаева, У.Т. Махажанова, М.А. Кантуреева, Г. Ускенбаева, Т.Н. Есикова

БІЛІМ БЕРУ НЕГІЗІНДЕ АУЫЛ ШАРУАШЫЛЫҒЫ КӘСІПОРЫНДАРЫНЫҢ ИНВЕСТИЦИЯЛЫҚ ТАРТЫМДЫЛЫҒЫН БАҒАЛАУ ӘДІСТЕМЕСІ.....235

А.Р. Оразаева, Д.А. Тусупов, В. Войчик , А.К. Шайханова, Г.Б. Бекешова

МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІМЕН СҮТ БЕЗІ ПАТОЛОГИЯСЫН ТИІМДІ АНЫҚТАУ...246

Б.Б. Оразбаев, Б.У. Асанова, Ж.Ж. Молдашева, Ж.Е. Шангитова

АЙҚЫНСЫЗДЫҚТА КОКСТЕУ РЕАКТОРЛАРЫНЫҢ ЖҰМЫС РЕЖИМДЕРІН КӨПКРИТЕРИЙЛІК ОПТИМИЗАЦИЯЛАУ ЕСЕБІНІҢ ҚОЙЫЛЫМЫ МЕН ОНЫ ШЕШУ ЭВРИСТИКАЛЫҚ ТӘСІЛІ.....258

Г.А. Салтанова, К.Б. Багитова, Г.А. Дашева, М.Е. Шангитова, Э.Г. Гайсина

УНИВЕРСИТЕТ КІТАПХАНАСЫНЫҢ АВТОМАТТАНДЫРЫЛҒАН АҚПАРАТТЫҚ ЖҮЙЕСІН ӘЗІРЛЕУ ЖӘНЕ ЕНГІЗУ: АҚПАРАТТЫҚ РЕСУРСТАРДЫ БАСҚАРУДЫ ОҢТАЙЛАНДЫРУ ЖӘНЕ ПАЙДАЛАНУШЫЛАРҒА ТИІМДІ ҚЫЗМЕТ КӨРСЕТУ.....269

Л.Т. Салыбек, К.Н. Оразбаева, В.Е. Махатова, Л.Т. Курмангазиева, Б.Е. Утенова

МҰНАЙДЫ АЛҒАШҚЫ ӨҢДЕУ ҚОНДЫРҒЫСЫ АТМОСФЕРАЛЫҚ БЛОГЫНЫҢ МОДЕЛЬДЕРІН ТҮРЛІ СИПАТТАҒЫ ҚОЛЖЕТІМДІ АҚПАРАТ НЕГІЗІНДЕ ҚҰРУ.....285

А. Сейтенов, Т. Жукабаева, С. Ал-Маджид

ЭЛЕКТРОНДЫҚ МЕДИЦИНАЛЫҚ ТӨЛҚҰЖАТЫ МЕН ТЕЛЕМЕДИЦИНА АҚПАРАТТЫҚ ЖҮЙЕСІНІҢ МОДЕЛІН ЖОБАЛАУ.....297

Г.Б. Турмуханова, А.А. Таутенбаева, Г.Т. Бекова, С.Б. Нугуманов, Я. Култан

ӘЛЕУМЕТТІК МЕДИА ҚАУЫМДАСТЫҚТАРЫНДАҒЫ ӨЗАРА ІС-ҚИМЫЛ АРҚЫЛЫ УНИВЕРСИТЕТ СТУДЕНТТЕРІНІҢ ЖҰМСАҚ ДАҒДЫЛАРЫН ҚАЛЫПТАСТЫРУ.....310

А.С. Тыныққұлова, А.В. Фаддеенков, А.А. Мұханова, А.У. Искалиева, Д.Б. Абулкасова

БЕЛГІСІЗДІК ЖАҒДАЙЫНДА ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫ ТАЛДАУ ЖӘНЕ ОҢТАЙЛАНДЫРУ: ЗАМАНАУИ ӘДІСТЕР МЕН ТЕХНОЛОГИЯЛАР.....325

Ж.Р. Умарова, Г.Ж. Ельбергенова, Н.С. Жуматаев, А.Х. Махатова, С.Б. Ботаева

МЕЗОСКОПИЯ ДЕҢГЕЙІНДЕГІ МОЛЕКУЛАЛЫҚ ЕЛЕКТЕРДЕГІ ЗАТ ТАСЫМАЛУЫН ЕСЕПТЕУ АЛГОРИТМІНІҢ ЗИЯЛДЫ ТАЛДАУЫ.....336

СОДЕРЖАНИЕ

Н. Абдразакулы, Л. Черикбаева, Н. Мукажанов, Ж. Алибиева

СОЗДАНИЕ ЭФФЕКТИВНОГО АЛГОРИТМА ОБРАБОТКИ ИЗОБРАЖЕНИЙ НА ОСНОВЕ АНСАМБЛЕВОГО ПОДХОДА.....7

Б.Т. Абыканова, А.А. Таутенбаева, А.Г. Амангосова, Г.Т. Бекова, А.Ж. Акматбекова

ИНТЕРАКТИВНЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В СОВЕРШЕНСТВОВАНИИ И РАЗВИТИИ САМОСТОЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ.....30

Ж.Ж. Ажибекова, Д.И. Усипбекова, Б.Н. Джаханова, К. Жыланбаева, Ә.Н. Тұрсун

УДАЛЕНИЯ ОБЛАКОВ И ТУМАННОСТЕЙ С КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ.....43

М. Айтимов, Г.Б. Абдикеримова, К.К. Макулов, Б.А. Досжанов, Р.У. Альменаева

ИССЛЕДОВАНИЕ ЭМОЦИОНАЛЬНОЙ ТОНАЛЬНОСТИ ТЕКСТА С ПРИМЕНЕНИЕМ АЛГОРИТМОВ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ.....57

А.Т. Акынбекова, А.А. Муханова, Salah Al-Majeed, Г.С. Алтаева

НЕЧЕТКИЕ МОДЕЛИ ПРИНЯТИЯ РЕШЕНИЙ ОЦЕНКИ СОЦИАЛЬНЫХ ПРОЦЕССОВ РАЗВИТИЯ РЕГИОНА.....69

К.М. Алдабергенова, А.Б. Касекеева, М.Ж. Айтимов, К.К. Дауренбеков, Т.Н. Есикова

СОВЕРШЕНСТВОВАНИЕ МАРКЕТИНГОВОГО УПРАВЛЕНИЯ ЛОГИСТИКОЙ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА.....85

А.Е. Абжанова, А.А. Быков, С.К. Сагнаева, Е.А. Абжанов, Д.И. Суржик

ОПТИМИЗАЦИЯ МОДЕЛИРОВАНИЯ ГРУНТА С УЧЕТОМ ПОДЗЕМНЫХ ГРУНТОВЫХ ВОД.....96

А.М. Бисенгалиева, А.У. Исембаева, Т.К. Душаева, Н.М. Алмабаева, Г.О. Ильясова

ОХВАТ КЛЮЧЕВЫХ СЛОВ С ПРИМЕНЕНИЕМ СЕМАНТИЧЕСКОГО АНАЛИЗА ДАННЫХ.....108

А.Х. Давлетова, Н.Н. Оразова, Ж.Б. Сайлау, Д.Н. Курмангалиева, Г.Л. Абдугалимов

ПУТИ ПОДГОТОВКИ УЧАЩИХСЯ НАЧАЛЬНЫХ КЛАССОВ К МЕЖДУНАРОДНОМУ ИССЛЕДОВАНИЮ PIRLS С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....120

Г. Есмагамбетова, А. Кубигенова, А. Актаева, И. Цэрэн-Онолт, М. Есмагамбет

МЕТОДЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ НА ОСНОВЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ.....137

Г.К. Ешмурат, Л.С. Каинбаева

МАТЕМАТИЧЕСКАЯ ТРЕВОЖНОСТЬ И ЕЁ ВЛИЯНИЕ НА КАРЬЕРУ БУДУЩИХ УЧИТЕЛЕЙ МАТЕМАТИКИ.....149

Т.К. Жукабаева, В.А. Десницкий, Е.М. Марденов

МЕТОДИКА СБОРА, ПРЕДОБРАБОТКИ И АНАЛИЗА ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ.....163

А.М. Джумагалиева, А.А. Шекербек, Ж.Ж. Хамитова, М. Свобода, С.А. Калдар

ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ С ПОМОЩЬЮ АДАПТИВНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АНОМАЛИЙ ПОСРЕДСТВОМ МАШИННОГО ОБУЧЕНИЯ.....177

А.А. Исмаилова, Г.Е. Мырзабекова, М.Ж. Базарова, Г.Ж. Нурова, Г.Т. Азиева

ПРОГНОЗИРОВАНИЕ ЦЕН НА ФОНДОВОМ РЫНКЕ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ

ГЛУБОКОГО ОБУЧЕНИЯ.....190

К. Кощанова, Ш. Сапарбайқызы, К.Е. Жангазакова, А.С. Сағынбай, Э. Куриэль-Марин

МАКСИМАЛЬНОЕ ИСПОЛЬЗОВАНИЕ ПОТЕНЦИАЛА ОБРАЗОВАНИЯ В STEM: ВКЛАД, ПРОБЛЕМЫ И СТРАТЕГИИ ДЛЯ УЛУЧШЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ.....205

А.А. Муханова, С.К. Кожукаева, Л.Г. Рзаева, Ж.Е. Доумчариева, У.Т. Махажанова

ПРИМЕНЕНИЕ И АНАЛИЗ МОДЕЛЕЙ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ СЕТЧАТКИ ГЛАЗА НА ОСНОВЕ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ.....218

Ә.Ж. Омуртаева, У.Т. Махажанова, М.А. Кантуреева, Г. Ускенбаева, Т.Н. Есикова

МЕТОДИКА ОЦЕНКИ ИНВЕСТИЦИОННОЙ ПРИВЛЕКАТЕЛЬНОСТИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ПРЕДПРИЯТИЙ НА ОСНОВЕ ПРЕДСТАВЛЕНИЯ ЗНАНИЙ...235

А.Р. Оразаева, Д.А. Тусупов, В. Войчик, А.К. Шайханова, Г.Б. Бекешова

ЭФФЕКТИВНОЕ ВЫЯВЛЕНИЕ ПАТОЛОГИИ МОЛОЧНОЙ ЖЕЛЕЗЫ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ.....246

Б.Б. Оразбаев, Б.У. Асанова, Ж.Ж. Молдашева, Ж.Е. Шангитова

ПОСТАНОВКА ЗАДАЧИ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ РЕЖИМОВ РАБОТЫ КОКСОВЫХ РЕАКТОРОВ В УСЛОВИЯХ НЕЧЕТКОСТИ И ЭВРИСТИЧЕСКИЙ МЕТОД ЕЕ РЕШЕНИЯ.....258

Г.А. Салтанова, К.Б. Багитова, Г.А. Дашева, М.Е. Шангитова, Э.Г. Гайсина

РАЗРАБОТКА И ВНЕДРЕНИЕ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УНИВЕРСИТЕТСКОЙ БИБЛИОТЕКИ: ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И ОБЕСПЕЧЕНИЕ ЭФФЕКТИВНОГО ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ.....269

Л.Т. Салыбек, К.Н. Оразбаева, В.Е. Махатова, Л.Т. Курмангазиева, Б.Е. Утенова

РАЗРАБОТКА МОДЕЛЕЙ АТМОСФЕРНОГО БЛОКА УСТАНОВКИ ПЕРВИЧНОЙ ПЕРЕРАБОТКИ НЕФТИ НА ОСНОВЕ ДОСТУПНОЙ ИНФОРМАЦИИ РАЗЛИЧНОГО ХАРАКТЕРА 285

А. Сейтенов, Т. Жукабаева, С. Ал-Маджид

ПРОЕКТИРОВАНИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТЕЛЕМЕДИЦИНЫ С ЭЛЕКТРОННОЙ МЕДИЦИНСКОЙ КАРТОЙ.....297

Г.Б. Турмуханова, А.А. Таутенбаева, Г.Т. Бекова, С.Б. Нугуманов, Я. Култан

ФОРМИРОВАНИЕ МЯГКИХ НАВЫКОВ СТУДЕНТОВ УНИВЕРСИТЕТА ПОСРЕДСТВОМ ВЗАИМОДЕЙСТВИЯ В СООБЩЕСТВАХ СОЦИАЛЬНЫХ СЕТЕЙ.....310

А.С. Тыныкулова, А.В. Фаддеенков, А.А. Муханова, А.У. Искалиева, А.Б. Абулкасова

АНАЛИЗ И ОПТИМИЗАЦИЯ УПРАВЛЕНИЯ РИСКАМИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ: СОВРЕМЕННЫЕ МЕТОДЫ И ТЕХНОЛОГИИ.....325

Ж.Р. Умарова, Г.Ж. Ельбергенова, Н.С. Жуматаев, А.Х. Махатова, С.Б. Ботаева

ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ АЛГОРИТМА РАСЧЕТА ПЕРЕНОСА ВЕЩЕСТВА В МОЛЕКУЛЯРНЫХ СИТАХ НА МЕЗОСКОПИЧЕСКОМ УРОВНЕ.....336

CONTENTS

N. Abdrazakuly, L. Cherikbayeva, N. Mukazhanov, Zh. Alibiyeva

CREATING AN EFFECTIVE IMAGE PROCESSING ALGORITHM BASED ON AN ENSEMBLE APPROACH.....7

B.T. Abykanova, A.A. Tautenbayeva, A.Г. Amangosova, G.T. Bekova, A.Zh. Akmatbekova

INTERACTIVE EDUCATIONAL TECHNOLOGIES IN IMPROVING AND DEVELOPING STUDENTS' AGENCY.....30

Zh.Zh. Azhibekova, D.I. Ussipbekova, B. Djakhanova, B.K. Zhylanbaeva, A.N. Tursun

REMOVING CLOUDS AND NEBULAE FROM SPACE IMAGES USING MACHINE LEARNING METHOD.....43

M. Aitimov, G.B. Abdikerimova, K.K. Makulov, B.A. Doszhanov, R.U. Almenayeva

STUDY OF THE EMOTIONAL TONE OF A TEXT USING MACHINE AND DEEP LEARNING ALGORITHMS.....57

A. Akynbekova, A. Mukhanova, Salah Al-Majeed, G. Altayeva

FUZZY DECISION MAKING MODELS FOR ASSESSING SOCIAL PROCESSES OF REGIONAL DEVELOPMENT.....69

K.M. Aldabergenova, A.B. Kassekeyeva, M. Aitimov, K. Daurenbekov, T.N. Esikova

IMPROVEMENT OF MARKETING MANAGEMENT OF LOGISTICS OF THE AGRICULTURAL COMPLEX.....85

A.E. Abzhanova, A.A. Bykov, S.K. Sagnaeva, E.A. Abzhanov, D.I. Surzhik

OPTIMIZATION OF SOIL MODELING WITH CONSIDERATION OF UNDERGROUND GROUNDWATER.....96

A.M. Bissengaliyeva, A.U. Issembayeva, T.K. Dushayeva, N.M. Almabayeva, G.O. Ilyassova

KEYWORD COVERAGE USING SEMANTIC DATA ANALYSIS.....108

A.Kh. Davletova, N.N. Orazova, ZH.B. Sailau, D.N. Kurmangalieva, G.L. Abdulgalimov

WAYS TO PREPARE PRIMARY SCHOOL STUDENTS FOR INTERNATIONAL PIRLS RESEARCH USING INFORMATION TECHNOLOGY.....120

G. Yesmagambetova, A. Kubigenova, A. Aktayeva, I. Tseren-Onolt, M. Esmaganbet

METHODS OF BIOMETRIC DATA PROTECTION BASED ON QUANTUM COMPUTING.....137

G.K. Yeshmurat, L.S. Kainbayeva

UNDERSTANDING MATH ANXIETY AND ITS IMPACT ON MATH EDUCATION STUDENTS' CAREERS.....149

T.K. Zhukabayeva, V.A. Desnitsky, E.M. Mardenov

A TECHNIQUE FOR COLLECTION, PREPROCESSING AND ANALYSIS OF DATA IN WIRELESS SENSOR NETWORKS.....163

A.M. Jumagaliyeva, A.A. Shekerbek, Zh.Zh. Khamitova, M. Svoboda, S. Kaldar

ENHANCING CYBERSECURITY WITH ADAPTIVE ANOMALY DETECTION SYSTEMS THROUGH MACHINE LEARNING.....177

A.A. Ismailova, G. Murzabekova, M.Zh. Bazarova, G.Zh. Nurova, G.T. Azieva

FORECASTING PRICES IN THE STOCK MARKET USING DEEP LEARNING METHODS.....190

G. Kochshanova, Sh. Saparbaykyzy, K.Y. Zhangazakova, A.S. Sagynbay, E. Curiel-Marin

MAXIMIZING THE POTENTIAL OF STEM EDUCATION: CONTRIBUTIONS, CHALLENGES, AND STRATEGIES TO IMPROVE LEARNING OUTCOMES.....205

A.A. Mukhanova, S.K. Kozhukaeva, L.G. Rzayeva, Zh.E. Doumcharieva, U.T. Makhazhanova

APPLICATION AND ANALYSIS OF DEEP LEARNING MODELS FOR DIAGNOSIS OF RETINAL DISEASES FROM MEDICAL IMAGES.....218

A. Omurtayeva, U. Makhazhanova, M. Kantureyeva, G. Uskenbayeva, T.N. Esikova

METHODOLOGY FOR ASSESSING THE INVESTMENT ATTRACTIVENESS OF AGRICULTURAL ENTERPRISES BASED ON THE PRESENTATION OF KNOWLEDGE.....235

A.R. Orazayeva, J.A. Tussupov, W. Wójcik, A.K. Shaikhanova, G.B. Bekeshova

EFFECTIVE DETECTION OF BREAST PATHOLOGY USING MACHINE LEARNING METHODS.....246

B.B. Orazbayev, B.U. Asanova, Zh.Zh. Moldasheva, Zh.E. Shangitova

FORMULATION OF THE PROBLEM OF MULTICRITERIAL OPTIMIZATION OF OPERATING MODES OF COKE REACTORS UNDER FUZZY CONDITIONS AND A HEURISTIC METHOD FOR ITS SOLUTION.....258

G.A. Saltanova, K.B. Bagitova, G.A. Dasheva, M.E. Shangitova, E.G. Gaisina

DEVELOPMENT AND IMPLEMENTATION OF AN AUTOMATED UNIVERSITY LIBRARY INFORMATION SYSTEM: INFORMATION RESOURCE MANAGEMENT OPTIMIZATION AND EFFECTIVE USER SERVICE PROVISION.....269

L. Salybek, K. Orazbayeva, V. Makhatova, L. Kurmangazieva, B. Utenova

DEVELOPMENT OF MODELS OF THE ATMOSPHERIC BLOCK OF A PRIMARY OIL PROCESSING PLANT BASED ON AVAILABLE INFORMATION OF VARIOUS NATURE.....285

A. Seitenov, T. Zhukabayeva, S. Al-Majeed

DESIGNING A MODEL OF A TELEMEDICINE INFORMATION SYSTEM WITH ELECTRONIC MEDICAL RECORD.....297

G.B. Turmukhanova, A.A. Tautenbayeva, G.T. Bekova, S.B. Nugumanov, K. Yaroslav

FORMATION OF UNIVERSITY STUDENTS' SOFT SKILLS THROUGH INTERACTION I N SOCIAL NETWORKING COMMUNITIES.....310

A.S. Tynykulova, A.V. Faddeenkov, A.A. Mukhanova, A. Iskaliyeva, D.B. Abulkassova

ANALYSIS AND OPTIMIZATION OF RISK MANAGEMENT IN CONDITIONS OF UNCERTAINTY: MODERN METHODS AND TECHNOLOGIES.....325

Zh. Umarova, G. Yelbergenova, N. Zhumatayev, A. Makhatova, S. Botayeva

INTELLIGENT ANALYSIS OF SUBSTANCE TRANSPORT ALGORITHM IN MOLECULAR SIEVES AT THE MESOSCOPIC LEVEL.....336

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)

Подписано в печать 15.06.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 2.

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