ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 4.

МАТЕМАТИКА, МЕХАНИКА И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

ПОДСЕКЦИЯ 4.1 МАТЕМАТИКА

204.	Galeeva Dilara Rustemovna	Investigation of the effect of variable viscosity on the velocity of droplet motion in a planar channel	2253
205.	Mukhutdinova Aygul Ayratovna	Flow of liquid with variable viscosity in a partially cooled channel with a cavity	2257
206.	Melsova Alua	Effective methods of data visualization and statistical analysis	2259
207.	Nurgali Nurmadi	Concave function inequalities for accretive dissipative matrices of the τ –measurable operators	2264
208.	Onerkhaan A.	The connection of h-amalgamation and joint continuation properties for h- inductive theories	2268
209.	Sadvakassov Aidos	On determinantal inequalities of τ -measurable operators	2266
210.	Абсаматова Адия Дауыловна	Дискретті жалпыланған Рисс потенциалының өспейтін алмастыруынан туындаған конустардың өзара байланысы	2272
211.	Айдос Айбүбі	Нұқсанды дифференциалдық теңдеулердің жалпыланған шешімдері	2273
212.	Алдомжарова Томирис Аблайқызы	Шенелмеген коэфициентті бір дифференциалдық операторды корректілік қасиеті	2276
213.	Альжанов Алдияр Маратович	Гармонический анализ на примере моделирования колебаний цен розничных товаров в Республике К азахстан	2279
214.	Бағымқызы Бағыжан	Эллис реологиясына негізделген сызықты емес дифференциалдық теңдеулердің аналитикалық және сандық шешімдері	2284

215.	Бақытжанова Гүлназ Нұрболқызы	Жоғарғы коэффициенті шексіздікте нөлге ұмтылатын үшінші ретті теңдеудің шешімділігі	2286
216.	Балагазинова Айым Муратовна	Дискретті салмақты лебег кеңістіктеріндегі дискретті салмақты максималды харди-литтлвуд операторы туралы	2288
217.	Гумарова Алия Балкыбековна	Дискретті Рисс потенциалының кейбір қасиеттері	2289
218.5	Есеналы Алмас	Кездейсоқ графтар теориясының аппроксимациялары	2292
219.6	Жолдасова Сымбат Жанбулатовна	Модули гладкости и коэффициенты рядов Фурье	2293
220.7	Исенова А.А., Багымкызы Б.	Айнымалы коэффициентті сызықты емес бюргер теңдеуі үшін қойылған бастапқы-шеттік есептің шешімділігі	2296
221.8	Қайратқызы Агнур	Салмақтық Соболев кеңістігінде дербес туындылы дисперсиялық теңдеудің бейсызық тегістігі	2297
222.9	Серимбетова Акниет Мураткызы	Весовая оценка для одного класса квазилинейных дискретных операторов	2300
223.0	Смагулова Маржан Толеугазиновна	Үйірткі операторының s сандары	2302
224.1	Утепбергенова Аида Ерболкызы	Математикалық статистика әдістері негізіндегі ҰБТ нәтижелері мен уақыт арасындағы байланыс	2304

225.1	Халыкберген Надияр	Интерполяционная теорема Марцинкевича-Кальдерона для дискретного пространства Лоренца	2307
226.2	Чаякова Аяулы Даулетқызы	Математикалық статистика әдістерін жаратылыстану ғылымдарында қолдану	2309

ПОДСЕКЦИЯ 4.2 МЕХАНИКА

227.1	Galeeva Dilara Rustemovna	Investigation of the effect of variable viscosity on the velocity of droplet motion in a planar channel	2316
228.2	Mukhutdinova Aygul Ayratovna	Flow of liquid with variable viscosity in a partially cooled channel with a cavity	2319
229.3	Абдибаттаева Айша Гизатхановна	Математическое моделирование распределение давление поверхность крыла	2322
230.4	Алпысбаев Нұрәділ Қанатұлы, Махмутов Тілеуқан Қанатұлы	Орта қашықтыққа арналған ұұа-ның аэродинамикалық сипатамаларын модельдеу	2325
231.5	Базарбаев Тамирлан	Конечно-элементный анализ несущей конструкции буровой установки	2330
232.6	Жанболат Әлихан Қанатұлы	Расчет и анализ аэродинамических характеристик автомобильного кузова	2334
233.7	Жәлел Әділғазы Әлиұлы	Уран өндіруде жер асты шаймалау әдісін сандық модельдеу	2337

234.8	Жуманбаева Айжан Сериковна	Численный расчет и сравнение моделей турбулентности при моделировании теплообмена в теплообменнике	2341
235.9	Калиаскер Нұрболат Серікұлы	Қабықша түтікшелі жылу алмастырғыш құбырларындағы бензол мен салқындатқыштың (судың) ағын режимдері мен параметрлерін анықтау	2345
236.0	Кәлімжан Әлия, Ерзат Мырзахан	Шаңсорғыш роботтың құрылымын жобалау	2348
237.11	Кенжехан Батырхан Ернатұлы, Тілеубаева Аружан Жомартқызы	Моделирование профиля крыла бпла в зависимости аэродинамических характеристик	2352
238.1	Маркова Лолита Валерьевна	Компьютерное моделирование падения капли на твердую поверхность в matlab	2357
239.1	Паклин Леонид Сергеевич	Анализ принципов регулирования режимов резонансных колебаний двухмассной вибрационной машины	2362
240.1	Рахимбеков Ислам Ерланович	Циклдік координаталық жүйелер үшін Раус әдісін қолдану	2365
241.1	Русланов Бекнур Русланович	Разработка конструкции багажной аэродромной тележки и расчет на прочность их элементов	2369
242.1	Тастан Мирас Нұрболатұлы	Өзен арнасын тазалау үшін гидроциклонды сорғылы қондырғылардың параметрлерін есептеу	2374
243.7	Тілеубаева Аружан Жомартқызы, Кенжехан Батырхан Ернатұлы	Численное моделирование течения жидкости вокруг колеблющейся стенки на програмном обеспечении ansys	2379

244. 8	Тулькибаев Чингис Куанышбаевич, Курманова Динара Есентаевна	Влияние граничных условий на теплообменный процесс в расчетах теплообменников	2382
245. 9	Чагин Даниил Михайлович	Влияние ударного взаимодействия на динамику горизонтальной двухмассной ударно-вибрационной площадки	2384

ПОДСЕКЦИЯ 4.3 МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

246.	Serikov Samat	Optimazation of algorithms for fingerprint search and matching using clustering and approximate nearest neighbor	2389
247.	Абат Дулат Ақниетұлы	Ейзенберг моделінің қиратушы толқын типті шешімдері	2393
248. 3	Абдреймова Айгерим Уриякизи	Сандық модельдеу әдістерін қолдана отырып, сызықты емес бөлшек спиндік жүйе үшін жаңа солитон шешімдерін әзірлеу	2396
249. 4	Алайдарова Мөлдір Мамырханқызы	Сандық модельдеуді қолдана отырып, күрделі сызықты емес спиндік жүйе Кауфман-Эккер теңдеуі үшін дәл оптикалық солитон құрылымдарын модельдеу	2400
250. 5	Алтынбек Ж., Алмахан Ер., Асилмаметов Б., Аманжол Ш., Акімхан А.	Числовая угадайка	2402
251. 6	Аскаров А., Әуезхан А., Ғазизханов Е., Баққали А., Сейтенова Б.	Қауіпсіз құпиясөз генераторы	2404
252. 7	Әбілхан Назым Ержанқызы	Есептеу тәсілімен сызықты емес бөлшек спиндік жүйелердің динамикалық теңдеуіне солитондық толқын құрылымын құру	2407

253.8	Байбатыров Мерхат Маликович	Разработка веб-приложения для учета и сравнения достижений студентов	2410
254.9	Бақытқан Д., Слямова А., Аширалиева А., Бүркітбай А.	Random модулі туралы	2412
255.0	Баубек Б., Нурханова А., Альмухамбетова А., Боранов Н., Бегалы Б.	Цезарь шифры туралы	2415
256.1	Беркімбай Ислам Жарасқанұлы	Бір солитондық модельдің дисперсиясыз шегі туралы	2419
257.2	Бисимбаев Рустем Ерланович	Нейросетевое моделирование в композиционных материалах	2421
258.3	Елеусіз Ақбөбек Мұратбекқызы	Моделирование выбросов и их снижения в ЕНУ	2426
259.1	Ергазиева Арина Гайдарқызы	Моделирование динамики развития Капчагайского водохранилища и прогнозирование с использованием искусственного интеллекта	2428
260.5	Ерғазы Жансая Нұрғазықызы	Жоғары ретті сызықты емес жүйелерді бекітілген уақытта орнықтандыру	2431
261.6	Жалбасов Абдирахим Шиндаулетович	Көшкіндерді зерттеу әдістері	2436
262.7	Жанатбек Нұрбақ Нұрланұлы	Использование алгоритмов машинного обучения в диджитал маркетинге	2441
263.8	Искакова Адина Серікқызы	Вилкоксон критерийін дәріхана бизнесінде машиналық оқыту арқылы қолдану	2444
264.9	Камал Жайна	DFS алгоритмін қолдану арқылы графтармен жұмыс істеудің тиімді әдістері	2449
265.2	Кәрғожа Арай Ардаққызы	Сызықты емес спиндік толқындарды модельдеу және динамикалық талдау	2451
266.1	Кішкене Жұлдыз Асылбекқызы	DEEPFAKE және жасанды интеллект: цифрлық манипуляцияны математикалық модельдеу және анықтау әдістері	2454
267.2	Мейірбек Құралай Айдынбекқызы	Мейрамхана бизнесіндегі жарнамалық тиімділіктің математикалық моделі	2459
268.3	Мұқиятұлы Еламан	Бөлшек ретті туындылы Камасса-Холм теңдеуі және оның шешімдері	2462

269. 4	Серік Сабыржан Еркінұлы	Вариациялық есептеу есептерінде функционалдық экстремумды табу үшін жасанды интеллект әдістерін қолдану	2466
270. 5	Сұлтанбеков Жандос Мұсабекұлы	Машиналық оқыту алгоритмдері арқылы жылжымайтын мүлікті бағалау туралы	2468
271. 6	Төлеубек Жібек Ерболқызы	Графтағы циклді іздеу	2472
272. 7	Узахбаев Имангали Хангелди улы	Дамбаларды нақты уақыт мезетінде модельдеу	2475

ПОДСЕКЦИЯ 4.4

МЕТОДИКА ПРЕПОДАВАНИЯ МАТЕМАТИКИ

533.	Абайұлы Есқанат	«Оқыту тиімділігін арттыру үшін практикалық мазмұны бар геометриялық есептерді қолдану»	2479
534.	Абдирова Кәмшат Махамбетиярқызы	7-9 сынып оқушыларының геометрия пәнінде функционалдық сауаттылығын арттырудың маңызы	2484
535.	Абдрахманова Жұпар Қабидоллақызы	Математикалық білім берудегі жасанды интеллект	2488
536.	Абдуллаева Амина Асанхановна	Математикалық біліктерді қалыптастыруда «тіреу белгілерін» ұтымды қолдану тәсілдері	2493
537.	Адібай Аяулым Таубайқызы	Математикада критикалық ойлауды дамытуға арналған креативті әдістер	2496
538.	Альбертқызы Бибі	Орта мектепте математиканы гуманитарлық пәндермен байланыстыра оқыту	2501
539.	Аманбай Меруерт Маликқызы	Geogebra пайдалану арқылы геометриялық салуларды жүргізу	2506
540.	Аманжолова Ажар Дастанқызы	«$(a \pm b)^2$ және $a^2 - b^2$ формулаларының геометриялық мағынасы»	2510
541.	Амангельдина Гульдана	Үлгерімі төмен оқушыларға арналған математиканы оқытуда кейбір тәсілдерді тиімді қолдану	2514

542.	Айбосын Гүлзия	Қытайдың математикалық олимпиадалық дайындық жүйесі және Қазақстан үшін оның әдістемелік бейімделуі	2518
543.	Аяпбергенова Аяна Женисовна	Интеграция искусства в сферу преподавания математики	2523
544.	Әлдиева Жұлдыз Әбдіқадырқызы	Математика пәнін оқытуда дамыта оқыту технологиясын пайдалану	2525
545.	Бақыт Ерқанат	Математикалық есептер арқылы оқушылардың	2531
546.	Барлыбай Ақниет	Сабақта оқушылардың белсенділігін арттыру үшін дайын сызба және модельдер бойынша тапсырмаларды қолдану	2533
547.	Батталов Суңғат	Көпжақтар қималарын мектеп геометрия курсында салу әдістемесі	2537
548.	Бахадир Ақтолқын Копжанқызы	Мектеп оқушыларының оқуының тиімділігін арттыру үшін математика сабағында сюжеттік есептерді пайдалану	2541
549.	Бекдаулетова Томирис	Математика сабағында әдістемелік нұсқауларды цифрлік форматта қолдану ерекшеліктері	2545
550.	Боранбаев Нұрқасым Өскенбайұлы, Сейтжанова Аяулым Маралқызы	Фактор топ және оның дербес жағдайлары	2550
551.	Дүйсенбаева Шұғыла Саматқызы	Математика сабағында өмір тәжірибесіне негізделген тапсырмалар	2554
552.	Ерболат Аружан	Математика сабағында 5–8 сынып оқушыларына арналған мәтіндік есептерді жүйелі түрде топтастыру және олардың тиімді шешу жолдарын қарастыру	2557
553.	Еримбет Дана Каиргалиқызы	Білім сапасын бағалаудың халықаралық зерттеулерінің математикалық сауаттылық тапсырмалары бойынша оқушыларды дайындау	2560
554.	Ермекбаев Айдос Елубаевич, Хасенова Тилеужан Сериковна	Методика преподавания математики для студентов обучающихся по программе foundation для подготовки к ент	2564

555.	Есентурова Акерке Халеловна	«Жасанды интеллект: математиканы оқытудың жаңа мүмкіндіктері»	2567
556.	Жәрдембек Ғалима	Мектеп бағдарламасының 8-9 сыныптарындағы математика сабағында цифрлық технологияларды қолдану әдістері	2570
557.	Жұмағазы Шұға	Күрделі математикалық ұғымдарды визуализациялау арқылы оқыту	2580
558.	Жұмахан Ақниет Оралбайқызы	Математикалық диктант: оқушылардың білімін бекітудің тиімді құралы	2585
559.	Ибадулла Шұғыла Айғалиқызы	«Проблемалық оқыту арқылы мектеп оқушыларының математика бойынша зерттеушілік дағдыларын жетілдіру»	2588
560.	Икрамов Ізет Сағатбекұлы	Орта мектепте алгебраны оқыту процесінде тіректік конспектіні пайдалану	2592
561.	Иманбетова Ақпейіл Мұратқызы	Дифференциалдық теңдеулерді мектеп оқушыларына жас ерекшеліктерін ескере отырып оқыту технологиялары	2596
562.	Калапбергенова Дана Бауыржановна	Биология студенттеріне жоғарғы математиканы оқытудың ерекшеліктері	2599
563.	Карагизова Даурия Ролланқызы, Даулетжан Диана Жасуланқызы	Геометрия пәнінде бір есепті әр түрлі әдістермен шешу	2602
564.	Каримова Акерке Нурболаткызы	Сызбалар арқылы математикалық есептерді модельдеу: оқытудағы жұмыс дәптерінің рөлі	2605
565.	Кеңес Гулден Жеңісбайқызы	Мектеп математика курсында теңсіздіктерді оқытудың маңызы	2606
566.	Кеңесбай Бақдәулет Нұржігітұлы	Бұрыш хордасы	2611
567.	Қабиден Қуаныш Ерланұлы	Индивидуальный анализ и рекомендации для учеников с использованием ии	2611
568.	Қалдыбек Асылжан Асылбекұлы	Дифференциалдық теңдеуді грин функциясы әдісімен шешуді оқытудың әдістемесі	2618
569.	Құлымбет Ақзер Төрегелдіқызы	Мектеп оқушыларының функционалдық сауаттылығын дамытудағы pisa	2622
570.	Құсайнова Айдана Қанатбекқызы	Оқушылардың математикалық қабілеттерін диагностикалау мен бағалау әдістері	2626

571.	Марден Аяулым Қайратқызы	Геометрия сабағындағы топтық жұмыс арқылы оқушылардың белсенділігі мен ойлау қабілетін дамыту	2630
572.	Мейманкулова Сабина	Мектеп геометрия курсындағы салу есептерінің маңыздылығы және факультативтік сабақтардағы қолданылуы	2634
573.	Мейрам Серікболсын	Арифметиканың негізгі теоремасы	2638
574.	Мухамедиярова Ақмарал Анарбекқызы	Сызбалар арқылы математикалық есептерді модельдеу: оқытудағы жұмыс дәптерінің рөлі	2641
575.	Мұрат Ақбөпе Әділханқызы	Декарт координат жүйесін оқыту: тиімді әдістер мен практикалық тапсырмалар	2644
576.	Наматулла Зарина	7-9 сынып алгебрасындағы “теңдеулер мен теңдеулер жүйесі” бөлімін тапсырмалар арқылы оқыту әдістемесі	2648
577.	Несиптаева Нурай Арнуровна, Турмухаметова Гульназ Кайрбековна	Использование ии в методике преподавания математики	2652
578.	Нұржан Мейір	Интерактивті технологияларды пайдалану арқылы математиканың логикалық негіздерін оқыту	2655
579.	Нұржанқызы Алтынай	10 сынып геометриясын оқытуда проблемалық оқыту технологиясының элементтерін қолдану және оған мысалдар	2660
580.	Орынбасар Жангүл Шоқанқызы	Көпмүшелер туралы олимпиадалық есептерді шешу әдістері	2663
581.	Омирсерик Султан	Геймификация в обучении математики в школе	2667
582.	Сабыров Фархат Ердосович	Стереометриялық есептерді шешуде жасанды интеллект моделін қолдану	2671
583.	Сайлау Ерлан Оразбайұлы, Мәдіханқызы Әлия	Оқушыларды олимпиадаға дайындаудағы диофант теңдеулерін шешу әдістері	2674
584.	Сафин Ақерке Мейірханқызы	Сингапурлық оқыту әдістемесі: 7-сыныптың алгебра сабағында «апгрейд 45 минут» моделін қолдану	2678

585.	Сеитханова Арна Медеткызы	«Алгебра және анализ бастамалары» курсында формулаларды түрлендіру әдістемесі	2683
586.	Сексенбай Айтолсын Бекзатқызы	«Жоғары математиканы оқыту үшін жасанды интеллект негізінде интерактивті оқу материалдарын жасау»	2686
587.	Сарсенбаева Ақниет	Математика пәнін оқытуда ar және vr технологияларын қолдану	2690
588.	Серік Мерей Әсетқызы	10-11 сыныптарда қазіргі заманғы цифрлық технологияларды пайдаланып математиканы оқытудың теориялық негіздері	2696
589.	Сәбит Елдана Сағидолақызы	Оқушылардың шығармашылық ойлауын қалыптастыру үшін парадоксалды есептерді пайдалану	2701
590.	Смат Жанерке Нұрланқызы	Рационал және иррационал енгізілген радикалдар: жіктелуі және әдістемесі	2704
591.	Сұлтанғазы Аружан Серікқызы	10-сынып математикасы негізінде инклюзивті білім беру теориясы мен практикасы	2707
592.	Сыздыкова Анар Жомартовна	Координаталық әдіс арқылы стереометрия есептерін шешу жолдары	2712
593.	Сыздыкова Анар Жомартовна	Ұбт-ға дайындық: координаталық әдісті тиімді пайдалану	2715
594.	Сырымқызы Мөлдір	Тарихи контекст негізінде қарапайым тригонометриялық теңдеулерді оқыту әдістемесі: теория және тәжірибе	2719
595.	Таджекеева Акмарал Рабаевна, Оспанова Карлыгаш Муратхановна	Математика және тарих пәндері интеграциясының маңызы мен артықшылықтары	2723
596.	Тасболат Актоты Ержановна	Visible thinking в преподаваниии математики: как сделать мышление учащихся видимым для повышения их понимания и навыков решения задач	2727
597.	Тубетова Малика Арманқызы	«Python негізіндегі интерактивті құрал жасау арқылы ықтималдық есептерін шешуді оқыту»	2730

598.	Тельманова Баян Жаркыновна	Математика сабақтарында виртуалды және аралас оқыту	2735
599.	Тиллабек Мөлдір	Мектеп курсында тригонометрияны оқытудың тиімді әдістемесі	2739
600.	Тлеухан Баян	Ою-өрнектер группасының кейбір қасиеттері	2744
601.	Турекасым Жанар Ибрагимқызы	Қысқаша көбейту формулаларының геометриялық мағынасы	2745
602.	Тынысбеков Арыстанбек Ардақұлы	Қолданбалы есептер негізінде комбинаториканы оқыту әдістемесі	2750
603.	Хасенова Дильназ Жандарбековна	Тригонометриялық теңсіздіктерді шешу әдістерінің тиімділігі мен кемшіліктері	2753
604.	Хусенбай Алина	Стереометриялық есептерді шығаруда компьютерлік бағдарламаларды қолдануға мұғалімдерді оқыту әдістемесі	2757
605.	Шамелкан Шұғыла	Әлеуметтік медиа мен жасанды интелекттің көпмүшеліктерді оқыту мен үйрету тәжірибесіне интеграциясы	2762

ПОДСЕКЦИЯ 4.5

КРИПТОЛОГИЯ

606.	Абдуалиев Алмас Оразалыұлы	Эдвардсдың эллипстік қисықтары	2765
607.	Бөрібай Мирас Мұқтарұлы	Полиалфавиттік Евклидтік шифрды криптоталдау	2767
608.	Джубатканов Куаныш	Эволюция машинного обучения в криптографии: от теории к постквантовой безопасности	2769
609.	Ельтаев Адильхан Уалиханович	Криптожүйелердегі қайталанбайтын шифрлаудың криптоанализі	2774

СЕКЦИЯ 5

МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ

ПОДСЕКЦИЯ 5.1 СОВРЕМЕННЫЕ МЕЖДУНАРОДНЫЕ ПРОЦЕССЫ

8. Giraud-Carrier C. G., Martinez T. R. An integrated framework for learning and reasoning.
9. Aslett L. J. M., Esperança P. M., Holmes C. C. Encrypted statistical machine learning: New privacy preserving methods.
10. Hosfelt D. Automated detection and classification of cryptographic algorithms in binary programs through machine learning.
11. Aslett L. J. M., Esperança P. M., Holmes C. C. A review of homomorphic encryption and software tools for encrypted statistical machine learning.
12. Yang C.-Y., Sahita R. Towards a resilient machine learning classifier: A case study of ransomware detection.
13. Wenger E., Chen M., Charton F., Lauter K. SALSA: Attacking lattice cryptography with transformers.
14. Kim B. D., Vasudevan V. A., Woo J., et al. CRYPTO-MINE: Cryptanalysis via mutual information neural estimation.
15. Frimpong E., Nguyen K., Budzys M., et al. GuardML: Efficient privacy-preserving ML services through hybrid homomorphic encryption.
16. Stevens S., Wenger E., Li C., et al. SALSA FRESCA: Angular embeddings and pre-training for ML attacks on learning with errors.
17. Shafran A., Malach E., Ristenpart T., Segev G., Tessaro S. Is ML-based cryptanalysis inherently limited?

ӘОЖ 004.056.55

Криптожүйелердегі қайталанбайтын шифрлаудың криптоанализі

Ельтаев Адильхан Уалиханович
Adilkhaneltaev05@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Мархабатов Н. Д.

Қазіргі ақпараттық қауіпсіздік саласында криптографиялық жүйелердің маңыздылығы артып келеді. Ақпарат алмасу барысында деректердің құпиялығын сақтау үшін әртүрлі шифрлау әдістері қолданылады. Соның ішінде қайталанбайтын шифрлау тәсілдері ерекше орын алады. Бұл әдістердің негізгі ерекшелігі – бірегей кілттер немесе кездейсоқ түрде өзгеретін шифрлау алгоритмдерін қолдануында.

Криптоанализ қайталанбайтын шифрлау жүйелерінің беріктігін бағалауға және олардың әлсіз тұстарын анықтауға бағытталған. Қайталанбайтын шифрлау әдістерін талдау барысында шифрланған мәтіннің кездейсоқтық дәрежесін бағалау үшін энтропия ұғымы қолданылады. Егер $H(C)$ – шифрланған мәтіннің энтропиясы, ал $H(K)$ – қолданылған кілттің энтропиясы болса, онда мінсіз шифрлау жағдайында:

$$H(C|K) = H(M)$$

мұнда M – ашық мәтін. Бұл теңдік шифрланған деректердің толықтай қорғалғанын және оларды кілтсіз ашу мүмкін еместігін білдіреді.

Криптоанализ әдістері жиілік талдау, белгілі ашық мәтін шабуылдары және сызықтық криптоанализ сияқты тәсілдерді қамтиды. Қайталанбайтын шифрлау әдістеріне қарсы шабуыл жасау кезінде негізгі қиындық – кілттің өзгермелілігі мен жоғары энтропия деңгейі болып табылады. Бұл факторлар криптожүйенің беріктігін арттырады.

Қорыта айтқанда, қайталанбайтын шифрлау әдістерін зерттеу көрсеткендей, мұндай тәсілдер деректерді қорғаудың жоғары деңгейін қамтамасыз етеді. Дегенмен, олардың практикалық

қолданылуы үшін есептеу ресурстарының көп мөлшері талап етіледі. Осыған байланысты, болашақта тиімді әрі ресурсты аз қажет ететін қайталанбайтын шифрлау алгоритмдерін жасау өзекті мәселе болып қала береді.

Қолданылған әдебиеттер тізімі

1. Salomaa A. Public-key cryptography. S. l.: Springer-Verlag, 1990.
2. Шнайер Б. Прикладная криптография. М.: Триумф, 2003.
3. Van der Waerden B. L. Algebra 1. S. l.: Springer-Verlag, 1971.
4. Lang S. Algebra. S. l.: Addison-Wesley Publ. Co., 1965.
5. Biham E. Differential cryptanalysis of the Data Encryption Standard / E.Biham, A.Shamir. S.l.: Springer-Verlag, 1993.
6. Агибалов Г. П.Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикл. дискрет. математика. 2008. № 1. С. 34–42.
7. Matsui M. Linear cryptanalysis of DES cipher (1) // Proc. of the 1993 Symp. on cryptography and information security, Japan, Jan. 28–30, 1993. S. l. P.
8. https://cyberleninka.ru/article/n/evklidovy-kriptosistemy
9. https://sciup.org/evklidovy-kriptosistemy-14320201

ӘОЖ 004.056.55

БЕРЛЕКЭМП АЛГОРИТМІ

Жуматаева Дильназ
dilnaz.zhumatayeva@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Е. Р. Байсалов

Кіріспе

Қазіргі заманғы ақпараттық технологиялардың қарқынды дамуы ақпаратты сақтау, беру және қорғау мәселелерін өзекті етеді. Цифрлық деректердің сенімділігі мен қауіпсіздігін қамтамасыз ету үшін түрлі математикалық әдістер мен алгоритмдер қолданылады. Солардың бірі — Берлекэмп алгоритмі.

Берлекэмп алгоритмі қателерді түзету кодтарында, криптографияда және үлкен деректерді өңдеуде кеңінен қолданылады. Бұл алгоритм негізінен ақырлы өрістер теориясына сүйенеді және оның көмегімен күрделі есептеулер оңай жүзеге асырылады. Ақпараттық қауіпсіздік тұрғысынан қарағанда, Берлекэмп алгоритмі кодтарды тиімді түрде құруға және қателерді анықтап, түзетуге мүмкіндік береді, бұл деректердің бұзылуын немесе өзгертілуін болдырмауға көмектеседі.

Қазіргі таңда киберқауіпсіздік мәселесі өте маңызды, өйткені шабуылдаушылар мәліметтерді бұрмалауға, өзгертуге немесе рұқсатсыз алуға тырысады. Осыған байланысты, Берлекэмп алгоритмі деректерді қорғаудың негізгі құралдарының бірі ретінде қарастырылады. Ол құпия ақпаратты шифрлау, кодтау, деректердің бүтіндігін сақтау және қателерді түзету сияқты салаларда қолданылады.

Бұл жұмыста Берлекэмп алгоритмінің теориялық негіздері, оның математикалық құрылымы, сондай-ақ ақпараттық қауіпсіздік саласындағы маңыздылығы қарастырылады. Сонымен қатар, оның криптография, кодтау теориясы, деректерді қорғау және сигналдарды өңдеу салаларындағы қолданылуы зерттеледі.

Негізгі бөлім.

1. Өрістер мен сақиналар теориясы және олардың Берлекэмп алгоритмімен байланысы

Алгебралық құрылымдар математика мен ақпараттық қауіпсіздіктің негізін қалаушы маңызды салалардың бірі болып табылады. Өрістер мен сақиналар теориясы көптеген алгоритмдердің, соның ішінде Берлекэмп алгоритмінің негізінде жатыр.

Өріс (Field) – бұл екі негізгі амалға (қосу және көбейту) жабық, олардың әрқайсысында сәйкесінше бейтарап элемент бар және әрбір элементке қатысты кері элемент бар алгебралық құрылым. Өрістер деректерді өңдеу мен криптографиялық жүйелердің негізін құрайды. Мысалы, ақырлы өрістер ($\mathbb{F}_2$, $\mathbb{F}_3$, ..., $\mathbb{F}_p$) криптография мен қателерді түзету кодтарында кеңінен қолданылады.

Сақина (Ring) – бұл қосуға және көбейтуге жабық алгебралық құрылым. Өрістен айырмашылығы, сақинада әрбір элемент үшін кері көбейту элементі міндетті түрде болмайды. Бірақ, сақина теориясы кодтау теориясында, қателерді түзету және ақпараттық қауіпсіздік салаларында маңызды рөл атқарады.

Берлекэмп алгоритмі осы алгебралық құрылымдармен тығыз байланысты, өйткені ол ақырлы өрістердің және многочлендер сақинасының негізінде жұмыс істейді. Бұл алгоритм ақырлы өрістерде орындалатын Галуа теориясына сүйене отырып, деректерді тиімді өңдеуге мүмкіндік береді.

2. Берлекэмп алгоритмі және оның ақпараттық қауіпсіздіктегі маңызы

Берлекэмп алгоритмі алғашында қателерді түзету кодтарында қолдану үшін жасалған, бірақ уақыт өте келе ол криптографияда, кодтау теориясында және сигналдарды өңдеуде қолданыла бастады. Оның негізгі мақсаты — берілген көпмүшеліктің минималды көпмүшелігін табу және сызықтық қайталанатын тізбектерді анықтау.

Берлекэмп алгоритмінің негізгі қадамдары:

1. Кіріс деректерді алу – көпмүшелік немесе тізбек беріледі.
2. Қайталанатын қатынастарды анықтау – берілген тізбектің қайталану үлгісі есептеледі.
3. Минималды көпмүшелікті құру – нәтижесінде ең қысқа сызықтық қатынас анықталады.

Бұл әдіс деректерді тиімді кодтауға және декодтауға көмектеседі, себебі ол қате түзету кодтарының құрылымын анықтауға мүмкіндік береді. Сонымен қатар, алгоритм ақпараттық қауіпсіздік саласында келесі бағыттарда қолданылады:

- Криптографияда – Берлекэмп алгоритмі Goppa кодтары мен RSA секілді шифрлау жүйелерінде қолданылады.
- Қателерді түзету кодтарында – ол BCH кодтарын және Reed-Solomon кодтарын есептеуде тиімді әдіс болып табылады.
- Цифрлық байланыс жүйелерінде – сигналдарды өңдеу, деректерді қысу және ақпараттық арналардың сенімділігін арттыру үшін пайдаланылады.

3. Берлекэмп алгоритмінің тиімділігі және артықшылықтары

Берлекэмп алгоритмінің басты артықшылықтарының бірі – оның есептеу тиімділігі. Егер басқа әдістер үлкен өлшемді матрицалармен жұмыс істеуді талап етсе, Берлекэмп алгоритмі сызықтық қайта өрнектеу арқылы күрделілікті төмендетеді.

Оның негізгі артықшылықтары:

1. Жылдам есептеу – үлкен өрістерде тиімді жұмыс істейді.
2. Қателерді түзету мүмкіндігі – кодтау теориясында маңызды рөл атқарады.
3. Криптографиялық тұрақтылық – көптеген шабуылдарға төтеп бере алады.

Қазіргі уақытта ақпараттық қауіпсіздік барған сайын маңызды бола түсуде. Сандық технологиялар дамыған сайын деректерді қорғау, шифрлау және қатені түзету әдістерінің қажеттілігі артып келеді. Берлекэмп алгоритмі үлкен деректердің сенімділігін арттыруға және ақпаратты қорғауға ықпал ететін маңызды құралдардың бірі болып табылады.

Қорытынды

Берлекэмп алгоритмі – ақпараттық қауіпсіздік, кодтау теориясы және сигналдарды өңдеу салаларында кеңінен қолданылатын қуатты әдістердің бірі. Ол өрістер мен сақиналардың алгебралық қасиеттеріне негізделген, бұл оны тиімді және сенімді құралға айналдырады.

Қазіргі заманғы деректерді қорғау жүйелерінде Берлекэмп алгоритмінің рөлі ерекше, себебі ол кодтардың құрылымын анықтауға, деректердің тұтастығын сақтауға және ақпараттық жүйелердің сенімділігін қамтамасыз етуге көмектеседі. Сондықтан бұл алгоритм ақпараттық қауіпсіздіктің ажырамас бөлігі ретінде зерттеліп, жетілдірілуі қажет.

Қолданылған әдебиеттер тізімі:

1. Smart N.P. Cryptography: An Introduction. – McGraw-Hill, 2003.
2. Peterson W.W., Weldon E.J. Error-Correcting Codes. – MIT Press, 1972.
3. MacWilliams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. – North-Holland, 1977.
4. Gallian J. Contemporary Abstract Algebra. – Cengage Learning, 2017.
5. Ван Лин. Кодирование информации и защита данных. – М.: Мир, 1982.
6. Кнуг Д. Теория кодирования. – М.: Радио и связь, 1987.
7. Hoffman K., Kunze R. Linear Algebra. – Prentice Hall, 1971.

ӘОЖ 004.056.55

АШЫҚ КІЛТТІ КРИПТОГРАФИЯЛЫҚ ХАТТАМАЛАРДА ГИПЕРЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫ ҚОЛДАНУ

Мұханбетқалиева Назерке Нұрланқызы
mykhanbetnaz@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекші - Мархабатов Н.Д

Кіріспе

Бүгінгі таңда ақпараттық технологиялар адам өмірінің барлық саласына еніп үлгерді. Мемлекеттік басқару, банк жүйесі, электрондық сауда, білім беру мен денсаулық сақтау – барлығы да деректерді өңдеу мен сақтауға тәуелді. Осы тұрғыдан алғанда, ақпараттың қауіпсіздігін қамтамасыз ету – өте өзекті мәселе. Ақпараттың құпиялылығы мен тұтастығын сақтау үшін криптография негізгі құрал ретінде қолданылады.

Криптография саласында әсіресе ашық кілтті жүйелердің рөлі ерекше. Ашық кілтті криптография деректерді қауіпсіз түрде шифрлауға, пайдаланушыны растауға және электрондық қолтаңбалар арқылы деректердің заңдылығын қамтамасыз етуге мүмкіндік береді. Соңғы жылдары бұл салада эллиптикалық және гиперэллиптикалық қисықтарға негізделген алгоритмдерге деген қызығушылық артып отыр.

Гиперэллиптикалық қисықтар – эллиптикалық қисықтардың жалпыланған нұсқасы. Олар математикалық тұрғыдан күрделірек болғанымен, қысқа кілттер арқылы жоғары деңгейдегі