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

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

қауіпсіздікті қамтамасыз ете алады. Осыған байланысты, мұндай қисықтарға негізделген криптографиялық алгоритмдер ресурсы шектеулі құрылғыларда – мысалы, смарт-карталар мен IoT жүйелерінде – қолдануға өте тиімді. Бұл бағыт әлі де зерттелу үстінде және болашақта кеңінен қолданылуы мүмкін.

Дәстүрлі криптографиялық әдістердің кейбір түрлері қазіргі талаптарға толық сай келмейді. Мысалы, RSA алгоритмі жоғары қауіпсіздік үшін өте ұзын кілттерді қажет етеді. Ал эллиптикалық қисықтар негізіндегі криптография бұл мәселені шешсе де, одан да тиімді әрі ықшам жүйелерге сұраныс артып келеді. Осы тұрғыдан гиперэллиптикалық қисықтар жақсы балама бола алады. Олар аз ресурспен үлкен қауіпсіздік ұсына отырып, заманауи криптожүйелердің маңызды құрамдас бөлігіне айналуы мүмкін. Сондықтан бұл тақырыпты зерттеу – бүгінгі ақпараттық қауіпсіздік талаптарына жауап беретін өзекті ғылыми міндет.

. Ашық кілтті криптографияның тарихы мен принциптері

Криптография – ақпаратты рұқсат етілмеген қол жеткізуден қорғау мақсатында шифрлау әдістерін зерттейтін ғылым саласы. Ол адамзат өркениетінің дамуымен бірге пайда болып, әскери, саяси және дипломатиялық қызметтердің маңызды құралына айналған. Алғашқы қарапайым шифрлар – Цезарь шифры, атбаш, скитала сияқты әдістер әскери хаттарды шифрлау үшін пайдаланылған.

Орта ғасырларда криптография тек жабық элита мен әскери басқарушылар арасында қолданылды. Қайта өрлеу дәуірінде Виженер шифры сияқты полиалфавиттік әдістер ұсынылды. Алайда бұл шифрлар да XX ғасырға дейін криптоанализге қарсы тұра алмайтын болды.

XX ғасыр криптографияны түбегейлі өзгертті. Әсіресе Екінші дүниежүзілік соғыста Энигма сияқты шифрлау құрылғылары және оларды бұзу үшін құрылған Bletchley Park орталығы математиктер мен инженерлердің осы салаға бет бұруына түрткі болды. Соғыстан кейін криптография әскери мақсаттан жалпы ақпараттық қауіпсіздікке кеңейе бастады [1].

Компьютерлердің пайда болуымен криптография енді математикалық теорияларға сүйене бастады. 1970-жылдары криптография мен ақпараттық технологиялар бір-бірімен тығыз байланыс орнатты. Бұл кезеңде криптография тек құпиялылық емес, тұтастық (integrity), аутентификация (authentication) және терістеуден қорғау (non-repudiation) ұғымдарын да қамтитын ғылым ретінде қалыптасты.

Асимметриялық криптография идеясының пайда болуы

1976 жылы Уитфилд Диффи мен Мартин Хеллман дәстүрлі криптожүйелердің негізгі әлсіздігі – құпия кілтті алмасу мәселесін шешу үшін жаңа әдіс ұсынды. Олар жария түрде таратылатын кілт арқылы шифрлау жүргізіліп, ал құпия кілт арқылы оны ашуға болатын жүйені сипаттады. Бұл жаңалық "New Directions in Cryptography" мақаласында алғаш рет ғылыми түрде дәлелденді [2].

Бұл идея асимметриялық криптография (немесе ашық кілтті криптография) деп аталып, революциялық жаңалық болды. Ол қауіпсіз байланыс орнату, кілт алмасу, қолтаңба қою сияқты мәселелердің шешімін ұсынды. Енді хабарлама жіберуші алушының ашық кілтін пайдаланып шифрлайды, ал алушы тек өзінің жабық кілтімен ғана оны аша алады. Бұл әдіс үшінші тараптың құпия кілтті ұрлау мүмкіндігін жоққа шығарады.

Ашық кілтті криптография екі негізгі процесс бойынша жұмыс істейді:

Жіберуші алушының ашық кілтін қолданып хабарламаны шифрлайды. Алушы бұл хабарламаны тек өзіне ғана белгілі жабық кілтпен шешеді. Бұл байланыс қауіпсіздігін қамтамасыз етеді, себебі үшінші тұлға хабарламаны оқи алмайды.

1. Сандық қолтаңба (электрондық қол қою):
   Қол қоюшы өз жабық кілтін қолданып хабарламаға қол қояды. Алушы қолтаңбаның шынайылығын тексеру үшін ашық кілтті пайдаланады. Осылайша, хабарламаның өзгермегені және нақты жіберушіден келгені дәлелденеді [3].

Жүйенің қауіпсіздігі екі маңызды қағидаға негізделген:

- Бір бағытты есептер – есептеу оңай, кері бағытта шешу қиын (мысалы, үлкен сандар көбейтіндісінен бастапқы көбейткіштерді табу).
- Жабық кілтті ашық кілт арқылы табу мүмкін емес (немесе өте қиын, практикалық тұрғыда шешілмейтіндей болуы керек).

Ашық кілтті алгоритмдердің математикалық негіздері: Ашық кілтті жүйелердің қауіпсіздігі келесі қиын есептерге сүйенеді:

— RSA алгоритмі – үлкен сандарды жай көбейткіштерге жіктеу есебіне негізделеді. Бұл алгоритмде екі үлкен жай сан таңдалып, олардың көбейтіндісі арқылы ашық және жабық кілттер генерацияланады [4].

— Diffie–Hellman кілт алмасу алгоритмі – дискреттік логарифм есебіне негізделген. Бұл алгоритмде екі тарап ортақ негіз (g) және модуль (p) арқылы кілтті қауіпсіз түрде бөлісе алады [5].

— ElGamal алгоритмі – дискреттік логарифмге негізделген, бірақ хабарламаны кездейсоқ элемент арқылы шифрлау арқылы қосымша қауіпсіздік ұсынады.

— Эллиптикалық қисықтар криптографиясы (ECC) – эллиптикалық қисықтардағы дискреттік логарифмнің шешілмейтіндігіне негізделеді. ECC қысқа кілттерді пайдалана отырып, RSA-мен бірдей немесе одан да жоғары қауіпсіздік деңгейін ұсынады [6].

— Гиперэллиптикалық қисықтар (HECC) – ECC-нің кеңейтілген нұсқасы. Олар күрделірек қисықтармен жұмыс істейді, бірақ ECC-мен салыстырғанда аз жад пен қысқа кілтпен жоғары қауіпсіздікті қамтамасыз етеді. HECC алгоритмдері кейінгі тарауларда тереңірек қарастырылады [7].

Ашық кілтті криптографияның қолдану аясы

Бүгінде ашық кілтті криптографиясыз заманауи цифрлық жүйелерді елестету қиын. Ол келесі салаларда кеңінен қолданылады:

— Электрондық коммерция: Интернет-дүкендер мен банктердің сайттары SSL/TLS хаттамалары арқылы пайдаланушылардың деректерін қорғайды. HTTPS протоколы осы хаттамаларға негізделген.

— Электрондық пошта қауіпсіздігі: PGP (Pretty Good Privacy) және S/MIME жүйелері электрондық хаттарға шифрлау мен қол қою механизмдерін ұсынады.

— Сандық қолтаңбалар және PKI: Мемлекеттік және заңдық құжаттарда цифрлық қол қою жүйелері заңды түрде дәлел рөлін атқарады.

— VPN және корпоративтік желілер: Ашық кілтті жүйелер арқылы ұйым ішіндегі деректер қауіпсіз байланыс арнасында жіберіледі.

— Блокчейн технологиясы: Криптовалюталарда транзакциялар ашық кілтті қолтаңбалар арқылы расталады.

— IoT және смарт құрылғылар: ECC және HECC аз жадты, энергиясы төмен құрылғыларда қауіпсіздік үшін тиімді шешім ретінде қолданылады.

— Актуалдылығы мен болашағы

Ашық кілтті криптографияның болашағы пост-кванттық криптографиямен тығыз байланысты. Себебі кванттық компьютерлердің дамуы RSA, ECC сияқты алгоритмдердің қауіпсіздігіне қауіп төндіруде. Осыған байланысты жаңа криптожүйелер – квантқа төзімді алгоритмдер, гиперэллиптикалық қисықтар, тор негізіндегі шифрлау секілді бағыттар белсенді зерттелуде [8].

Ашық кілтті жүйелердің архитектурасы, есептеу тиімділігі, және қауіпсіздік деңгейін арттыру мақсатында жаңа математикалық негіздер мен криптографиялық схемалар құрылуда.

Ашық кілтті криптография – тек шифрлау емес, бүкіл ақпараттық қауіпсіздік архитектурасының негізі. Оның тарихи қалыптасуы мен ғылыми негізделуі бүгінде жоғары технологиялық жүйелерде, электрондық үкіметтерде, қаржы секторында және коммуникацияда кеңінен қолданылады.

Ашық кілтті жүйелер — қауіпсіз цифрлық болашақтың негізі. Дегенмен, бұл жүйелердің сенімділігі тікелей математикалық модельдер мен қолданылатын есептердің күрделілігіне тәуелді. Сондықтан қазіргі таңда гиперэллиптикалық қисықтар сияқты жаңа криптографиялық тәсілдерге бет бұру – уақыт талабы.

Гиперэллиптикалық қисықтар — алгебралық қисықтардың күрделі және кеңейтілген түрі, олар эллиптикалық қисықтардың жалпыланған моделі болып табылады. Бұл қисықтар криптографияда салыстырмалы түрде жаңадан қолданыла бастағанымен, олардың математикалық зерттелуі XIX ғасырда басталған.

Гиперэллиптикалық қисықтар — алгебралық қисықтардың эллиптикалық қисықтардан кейінгі табиғи жалғасы болып табылады. Бұл қисықтар түрі алгебралық геометрияның бір тармағы ретінде зерттеліп, соңғы жылдары криптографияда қолданыла бастаған. Гиперэллиптикалық қисықтар эллиптикалық қисықтар секілді дискреттік логарифм есебіне негізделген, алайда олардың құрылымы анағұрлым күрделірек.

Математикалық тұрғыдан гиперэллиптикалық қисықтар былай анықталады:

$$C: y^2 + h(x)y = f(x) \qquad (1)$$

мұндағы f(x) – дәрежесі 2g+1 немесе 2g+2 болатын көпмүшелік, ал h(x)– дәрежесі ≤g болатын көпмүшелік, және бұл теңдеу F_q шектеулі өрісінде анықталған. Егер h(x)=0 болса, қисық келесі қарапайым формаға келеді:

$$C: y^2 = f(x) \qquad (2)$$

Мұндағы g — қисықтың роды (genus). Егер g=1 болса, ол эллиптикалық қисыққа сәйкес келеді. Ал g≥2 болғанда – бұл гиперэллиптикалық қисық деп аталады [9].

Гиперэллиптикалық қисықтардың құрылымдық ерекшелігі – олардағы криптографиялық операциялар жәй нүктелермен емес, дивизорлармен (divisors) орындалады. Бұл оларды күрделендіреді, бірақ сол арқылы жоғары қауіпсіздік деңгейін қамтамасыз етеді.

Род (genus) ұғымы және оның рөлі

Род – алгебралық қисықтың күрделілігін сипаттайтын маңызды инвариант. Геометриялық тұрғыда род қисықтың «тесіктерінің» санына сәйкес келеді. Мысалы, эллиптикалық қисық – бұл роды 1 болатын қисық, ал гиперэллиптикалық қисықтарда g≥2.

Криптографияда родтың келесі маңызы бар:

— Род жоғарылаған сайын, криптографиялық кілттер саны артады, яғни қауіпсіздік кеңістігі үлкейеді;

— Род артқан сайын есептеу қиындайды, бірақ кейбір жағдайларда аз биттік параметрлермен жоғары қауіпсіздікке қол жеткізуге болады;

— Род g=2 және g=3 мәндерінде HECC (HyperElliptic Curve Cryptography) криптожүйелері өнімділігі мен қауіпсіздігі бойынша ECC-ге (Elliptic Curve Cryptography) бәсекелес бола алады [10].

Гиперэллиптикалық қисықтарды қолданғанда, көбіне g≤4 таңдалады, себебі одан жоғары мәндерде есептеу шығындары артып, практикалық тиімділігі төмендейді.

Дивизорлар және якобиан топтары

Гиперэллиптикалық қисықтардағы операциялар нүктелерде емес, дивизорларда орындалады. Дивизор – қисықтағы нүктелердің формальды бүтін сандармен алынған жиынтығы:

$$D = \sum n_i P_i \qquad (3)$$

мұндағыP_i— қисық нүктелері,n_iZ

Дивизорлардың жиынтығы Div(C) деп аталады. Тек нөлдік дәрежелі дивизорлар ғана криптографиялық мақсатта қолданылады, олардан құралған топ жейкобиан тобы (Jacobian group) деп аталады:

$$Jac(c) = Div^0(C)/Prin(C) \qquad (4)$$

Жейкобиан тобы – абелдік топ, мұнда қосу, кері элемент табу, кратный қосу секілді операциялар жасалады. Жейкобиан топтағы элементтер Mumford өкілдігінде беріледі:

D=(u(x),v(x)),мұндағыu(x)-мономиальды көпмүшелік, v(x)–төмен дәрежелі

Криптографиялық тұрғыда осы дивизорлар құпия кілт, ашық кілт және қолтаңба ретінде қызмет етеді [11].

Гиперэллиптикалық қисықтардағы арифметика: Cantor алгоритмі

Дивизорлармен жұмыс істеу үшін Cantor алгоритмі қолданылады. Бұл алгоритм екі дивизорды қосып, нәтижесін стандартты (Mumford) формаға келтіруге мүмкіндік береді. Оның негізгі кезеңдері:

1. Екі дивизор беріледі:

$$D_1 = \big(u_1(x), u_1(x)\big), D_2 = \big(u_2(x), u_2(x)\big), \qquad (4)$$

2. Көпмүшеліктер арқылы операция жасалады: $u = u_1.u_2, u = (u_1u_2 + u_2u_1)\mathrm{modu}$
3. Редукция (қысқарту) қадамы – алынған дивизорды қарапайым формаға келтіру үшін:

$$u' = \frac{u}{\gcd(u, u^2 - f)}, u' = -u \; mod \; u' \qquad (5)$$

4. Нәтижесінде алынған (u′,v′) — қосындының канондық түрі

Бұл операциялар эллиптикалық қисықтағы нүктелер қосу сияқты жұмыс істейді, бірақ есептеу жағынан күрделірек. Алайда қысқа кілттер қолдану арқылы өнімділікті жоғалтпай, қауіпсіздікті арттыруға болады [12].

Гиперэллиптикалық қисықтар — қазіргі криптографиядағы перспективалық бағыттардың бірі. Олардың математикалық құрылымы күрделі болғанымен, олар жоғары қауіпсіздік, қысқа кілттер, және аз ресурспен жұмыс істеу сияқты маңызды артықшылықтарға ие. HECC алгоритмдерінің математикалық негізі ретінде жейкобиан топтары, дивизорлар теориясы және Cantor алгоритмі қолданылады.

Криптографиядағы гиперэллиптикалық қисықтарды қолдану қазіргі таңда шектеулі болғанымен, зерттеулер мен тәжірибелік енгізулер олардың болашағы зор екенін көрсетеді. Осы қисықтарға негізделген жүйелердің нақты хаттамаларға енгізілуі келесі тарауда қарастырылады.

Пайдаланылған әдебиеттер

1. Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication. Scribner.

2. Diffie, W., & Hellman, M. (1976). "New Directions in Cryptography." IEEE Transactions on Information Theory, 22(6), 644–654.
3. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
4. Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the *ACM*, 21(2), 120–126.
5. Stinson, D. R. (2006). Cryptography: Theory and Practice. CRC Press.
6. Koblitz, N. (1987). "Elliptic Curve Cryptosystems." Mathematics of Computation, 48(177), 203–209.
7. Blake, I. F., Seroussi, G., & Smart, N. P. (1999). Elliptic and Hyperelliptic Curve Cryptography. Cambridge University Press.
8. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography. Springer.
9. Galbraith, S. D. (2012). Mathematics of Public Key Cryptography. Cambridge University Press.
10. Enge, A. (1999). Elliptic and Hyperelliptic Curve Cryptography: Algorithms and Implementation. Springer.
11. Koblitz, N., & Menezes, A. (2000). "Hyperelliptic Cryptosystems." Designs, Codes and Cryptography, 19(2–3), 197–210.
12. Lange, T. (2001). Efficient Arithmetic on Hyperelliptic *Curves*. PhD Dissertation, Universität Essen.
13. Blake, I. F., Seroussi, G., & Smart, N. P. (1999). Elliptic and Hyperelliptic Curve Cryptography. Cambridge University Press.
14. Hankerson, D., Vanstone, S., & Menezes, A. (2004). Guide to Elliptic Curve Cryptography. Springer.

ӘОЖ 004.056.55

БЛОКЧЕЙН ЖҮЙЕЛЕРІНДЕ КӨПФАКТОРЛЫ АУТЕНТИФИКАЦИЯНЫҢ ТИІМДІЛІГІН АРТТЫРУ ҮШІН МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕР МЕН АЛГОРИТМДЕР.

Өтепберген Ақтілек Дінмұхамбетқызы
dinmukambetkyzy@icloud.com
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Жетписбаев Д.

Кіріспе

Үздіксіз дамып келе жатқан цифрлық ландшафтта блокчейн технологиясы әртүрлі секторларда қауіпсіздікті, ашықтықты және тиімділікті қамтамасыз ететін революциялық күш ретінде пайда болды. Осы технологияның маңызды құрамдас бөлігі болып табылатын блокчейн қауіпсіздігі блокчейн желілерін зиянды шабуылдардан және рұқсатсыз кіруден қорғауға арналған киберқауіпсіздік принциптерінің, құралдарының және ең жақсы тәжірибелерінің кешенді жиынтығын қамтиды. Блокчейннің орталықтандырылмаған табиғаты қауіпсіздіктің өзіндік артықшылықтарын ұсынса да, ол бірегей қиындықтарды да тудырады. Блокчейн қауіпсіздігінің қыр-сырын түсіну оның әлеуетін пайдалану және оны