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

ӘОЖ 004.056.55

ИНТЕРНЕТ-КОММЕРЦИЯ ҮШІН ЗАМАНАУИ ДЕРЕКТЕРДІ ҚОРҒАУ ПРОТОКОЛДАРЫНЫҢ ТИІМДІЛІГІ

Серікбай Мәншүк Қуанышқызы
srmonojserikbai@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Мархабатов Н. Д.

Кіріспе

Кең таралған цифрландыру дәуірінде құпия ақпаратты қорғау және деректердің құпиялылығын қамтамасыз ету қажеттілігі бірінші орынға шықты. Криптография - қауіпсіз байланыс туралы ғылым, ол деректерді рұқсатсыз кіруден және зиянды шабуылдардан қорғауда маңызды рөл атқарады. Дәстүрлі криптографиялық жүйелер тиімді болғанымен, Интернет заттары (IoT) құрылғылары, ендірілген жүйелер және сымсыз сенсорлық желілер сияқты ресурстары шектеулі орталарда іске асырылған кезде, айтарлықтай қиындықтар туғызады. Бұл құрылғылар біздің күнделікті өмірімізде кең таралғандықтан, олардың шектеулі есептеу қуаты, жады және энергетикалық ресурстары оларды қауіпсіздік қатерлеріне осал етеді.

Осы қиындықтарды шешу үшін зерттеушілер мен практиктер перспективті шешім ретінде эллиптикалық қисықтардағы криптографияға (ECC)[1] жүгінді. ECC – ақырлы өрістерде эллиптикалық қисықтардың алгебралық қасиеттерін пайдаланатын ашық кілтті криптографиялық схема. ECC негізгі принципі - оның қауіпсіздігінің негізін құрайтын эллиптикалық қисықтардағы сызықтардың дискретті логарифмдік есептерін шешудің қиындығында жатыр. RSA және DSA сияқты дәстүрлі криптожүйелермен салыстырғанда, ECC анағұрлым қысқа кілт өлшемдері бар баламалы қауіпсіздікті ұсынады, бұл оны ресурстары шектеулі орталар үшін өте қолайлы етеді.[2]

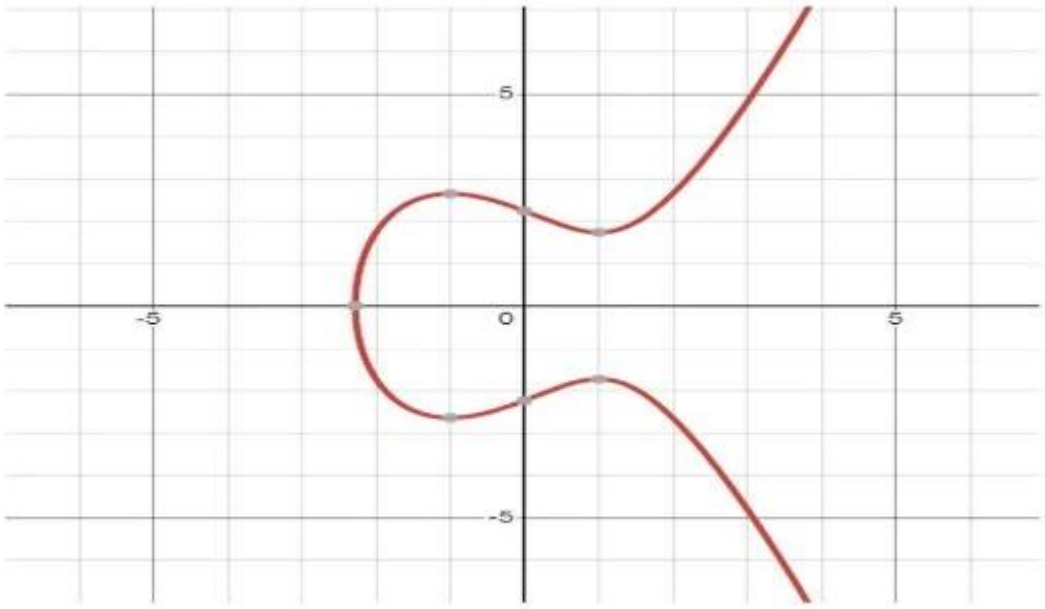
Ашық кілтті криптография 1970 жылдары ойлап табылды. Бұл дәстүрлі түрде компьютерлік және ақпараттық қауіпсіздік жүйелерін құру үшін математикалық негіз ретінде пайдаланылған асимметриялық криптографиялық алгоритмдер. Ашық кілтті криптографияны дамыту процесінде бір жақты функциялар деп аталатын математикалық функциялардың бірнеше кластары ашылды. Оларға, атап айтқанда, жай санды дәрежеге дейін көтеру, эллиптикалық қисықтарды көбейту және т.б. жатады. Қайтымсыздық, мұндай функциялардың тікелей мәндері өте қарапайым есептелетінін білдіреді, бірақ кері мәндерді есептеу іс жүзінде мүмкін емес. Бір жақты функцияларға негізделген сандық шифрлау және криптографиялық қауіпсіз электрондық қолтаңбалар үшін біршама алгоритмдер әзірленді. Соның бірі Диффи-Хеллман алгоритмі. Диффи-Хеллман - бұл екі тарапқа қауіпті арна арқылы ортақ құпия кілтті орнатуға мүмкіндік беретін жаңа криптографиялық протокол. Бұл алмасу әдісі - қоғамдық желілер арқылы, қауіпсіз байланысты қамтамасыз ету арқылы криптография саласында төңкеріс жасады. 1976 жылы әзірленген алғашқы ашық кілтті хаттамалардың бірі және бүгінгі күнге дейін кеңінен қолданылады. Ол Уитфилд Диффи мен Мартин Хеллманның есімімен аталған. Екеуі де қоғамда айрықша із қалдырған көрнекті криптографтар, ашық кілтті криптографияны ойлап тапқан үш адамдық командаңың бір бөлігі болды. Диффи-Хеллманның күшін эллиптикалық қисықтардағы криптографияның талғампаздығымен үйлестіре отырып,

бізде ақпаратымызды қорғау үшін бұзылмайтын құлыптың негізі - Эллиптикалық қисықтардағы Диффи-Хеллман протоколы(ECDH) бар.

Эллиптикалық қисықтардағы Диффи-Хеллман (ECDH) – әрқайсысында ашық-жеке кілт жұбы бар екі тарапқа қауіпті арна арқылы ортақ құпияны орнатуға мүмкіндік беретін негізгі келісім хаттамасы[3]. Бұл зерттеу жұмысы ресурсы шектеулі орталар үшін эллиптикалық қисықтардағы криптографияны пайдалана отырып, қауіпсіз кілт алмасуды тиімді енгізу нәтижелерін ұсынады, әсіресе көлік желілеріндегі басқару блоктары мен сенсорлары.

Эллиптикалық қисық криптографияны (ECC) алғаш рет Виктор Миллер және Нил Коблиц 1980 жылдардың ортасында ұсынған және жетілген ашық кілтті криптографиялық жүйеге айналдырған. Дәстүрлі әріптестерімен салыстырғанда, ECC анағұрлым кішірек кілттерді пайдалана отырып бірдей қауіпсіздік деңгейін ұсынады. Бұл жылдам есептеулер мен жадты, қуатты және өткізу қабілеттілігін үнемдеуге әкеледі, олар әсіресе шектеулі орталарда маңызды. Неғұрлым маңыздысы, ECC-тің бәсекелестерінен артықшылығы көп, өйткені қауіпсіздік қажеттіліктері уақыт өте келе артып келеді. Жақында Ұлттық стандарттар және технологиялар институты (NIST) АҚШ үкіметінің пайдалануы үшін ECC-ті мақұлдады.

Эллиптикалық қисық криптографиясы - ақырғы өрістерде анықталған эллиптикалық қисықтардың математикалық қасиеттеріне негізделген. Бұл бөлім эллиптикалық қисықтардың алгебралық құрылымын және дискретті логарифм есебін қоса алғанда, ECC негізін құрайтын негізгі ұғымдарға шолу жасайды.



1-сурет. $y^2 = x^3 - 3x + 5$

Эллиптикалық қисық Диффи-Хеллман (ECDH) кілттер алмасуы

Диффи-Хеллманның эллиптикалық қисығы – екі тарапқа қауіпті байланыс арнасы арқылы ортақ құпияны қауіпсіз орнатуға мүмкіндік беретін негізгі алмасу алгоритмі. Ол алдыңғы тарауда айтылған эллиптикалық қисықтардағы дискретті логарифмдік есептерді шешудің есептеу қиындығына негізделген. ECDH қазіргі заманғы криптографиялық хаттамаларда тиімділігі мен күшті қауіпсіздік қасиеттеріне байланысты кеңінен қолданылады. Процесс төменде қысқаша қорытындыланады.

G эллиптикалық қисығының генератор нүктесі болсын :

1. Алиса жеке кілтін dA *модулі* n бүтін сандар жиынынан таңдайды және олардың ашық кілтін QAG *санын* жеке кілтімен көбейту арқылы жасайды, $dA \in \mathbb{Z}n$,$QA=dA\times G$
2. Боб өзінің жеке кілтін таңдай отырып, бірдей процесті орындайды dB және өзінің жеке кілтін есептейді QB.
3. Алиса мен Боб ашық кілттерін алмастырады.
4. Алиса $SA=dA\times QB$ есептейді.
5. Боб $SB=dB\times QA$ есептейді.
6. Эллиптикалық қисық арифметикадағы нүктені скалярға көбейту коммутативті болғандықтан, екі тарап бірдей ортақ құпияға келеді $SA=SB=S$.

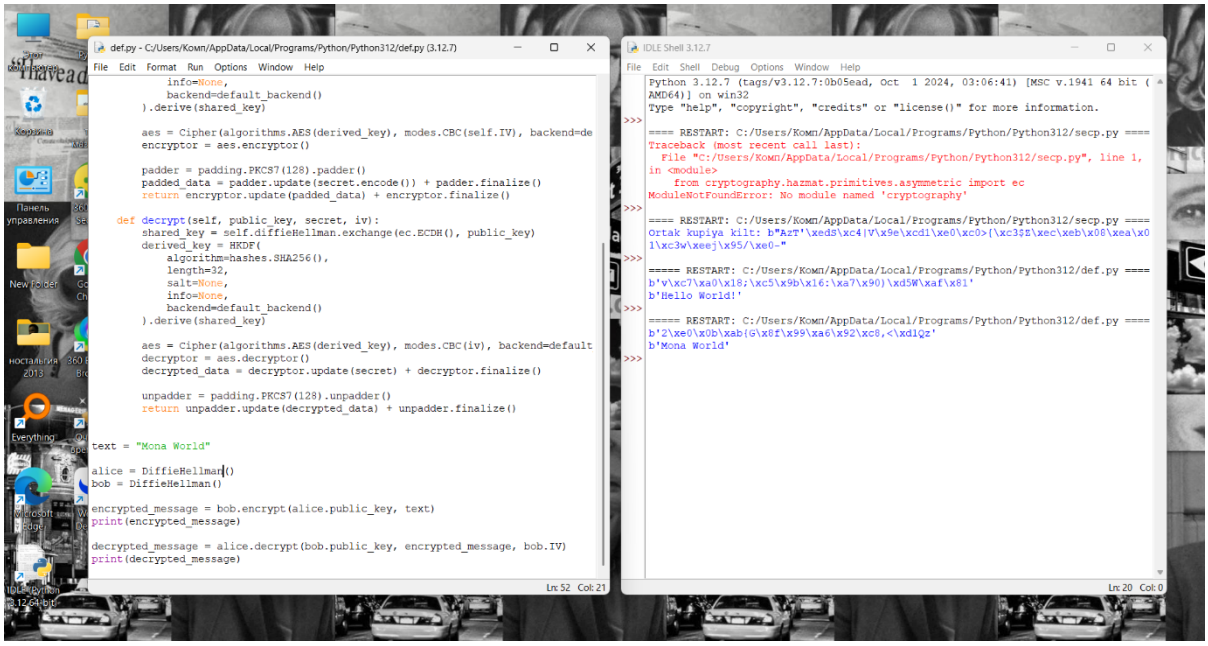
ECC қауіпсіздіктің негізгі артықшылықтарының бірі оның дәстүрлі криптожүйелермен салыстырғанда анағұрлым кішірек кілт өлшемдері бар баламалы қауіпсіздікті ұсына алуында жатыр. Мысалы, 256 биттік ECC кілті 3072 биттік RSA кілтімен бірдей қауіпсіздік деңгейін қамтамасыз етеді, нәтижесінде жад пен есептеу талаптары төмендейді [2]. SafeCurves [4] дискретті логарифм есептерінен тыс ECC қауіпсіздігін қамтамасыз ету үшін критерийлер жинағын ұсынады және осы критерийлерге қарсы әртүрлі қисықтарды бағалайды. Бұл нақты іске асыру үшін қисық сызықтарды таңдау кезінде тамаша ресурс.

NIST P-256, сондай-ақ secp256r1 ретінде белгілі, криптографиялық қолданбаларда, әсіресе Transport Layer Security, HTTPS және цифрлық қолтаңбалар сияқты хаттамаларда жиі қолданылатын эллиптикалық қисықтардың бірі. NIST өзінің Suite B криптографиялық стандарттарының бөлігі ретінде анықтаған.Ол қауіпсіздік пен тиімділік арасындағы тепе-теңдікті ұсынады, бұл оны ашық кілтті криптографияны қажет ететін қолданбалардың кең ауқымы үшін қолайлы етеді. Бірнеше зерттеулері әртүрлі контексттерде NIST P-256 қауіпсіздігі мен өнімділігін бағалады. Рыза және т.б. [5] эллиптикалық қисықтардың қауіпсіздігін, соның ішінде NIST P-256 ықтимал шабуылдарға қарсы бағалады және бұл қисықтар практикалық пайдалану үшін жеткілікті қауіпсіздікті қамтамасыз етеді деген қорытындыға келді. Гура және т.б. [6] ендірілген жүйелердегі эллиптикалық қисық криптографияның өнімділігін талдап, NIST P-256 ресурсы шектеулі құрылғылар үшін қауіпсіздік пен тиімділік арасындағы жақсы теңгерімді ұсынатынын анықтады.

secp256k1 эллиптикалық қисық сызығы, әсіресе Bitcoin [7] сияқты криптовалюталар саласында айтарлықтай беделге ие болды . Бұл қисықтың теңдеуі: $y^2 = x^3 + 7$

Secp256k1-дің көрнекті ерекшеліктерінің бірі - оның Bitcoin криптографиялық схемасында ашық-жеке кілт жұптарын генерациялау үшін негізгі эллиптикалық қисық ретінде қабылдау болып табылады. Биткоинның қауіпсіздігі - негізінен желідегі транзакциялардың тұтастығы мен құпиялылығын қамтамасыз ететін secp256k1 криптографиялық қасиеттеріне сүйенеді.

Енді осы secp256k1-ді пайдаланып Python тілінде ECDH алгоритмін енгізейік.



Енгізілген құрылғыларға арналған криптографиялық алгоритмдерді таңдау қауіпсіздік, өнімділік, жадты пайдалану және қуат тұтыну арасындағы нәзік тепе-теңдікке байланысты. NIST қисықтары және secp256k1 сияқты кеңінен қолданылатын басқа қисықтар стандартталған қауіпсіздік кепілдіктерін ұсынса да, Curve25519 орындау уақыты, жадты пайдалану және қуат тұтыну тұрғысынан жоғары, бұл ресурс шектеулі орталар үшін тартымды таңдау жасайды. Curve25519 енгізу арқылы дизайнерлер мен инженерлер қауіпсіздік пен ресурс тиімділігі арасындағы теңгерімге қол жеткізе алады, бұл ресурс шектеулі орталарда қауіпсіз криптографиялық шешімдерді қолдануға мүмкіндік береді.

Эллиптикалық қисықтардағы Диффи-Хеллман протоколын есептеу ресурстары мен өткізу қабілеттілігін пайдалану тұрғысынан жоғары тиімді.Оның математикалық құрылымының талғампаздығы кілттерді генерациялау және алмасу процестерін жеңілдетуге мүмкіндік береді, бұл оны IoT құрылғылары мен мобильді қосымшалар сияқты ресурстары шектеулі орталар үшін өте қолайлы етеді.Үздіксіз зерттеулер мен әзірлемелердің арқасында ECDH болашағы үлкен үміт береді, бұл біздің деректеріміздің пайда болатын қауіп қатерлерге қарсы қорғалуын қамтамасыз етеді.

Қолданылған әдебиеттер тізімі

1. Коблиц, Н. Эллиптикалық қисық криптожүйелер. Математика. Есептеу. **1987** , 48 , 203–209. [**Google Scholar**]
2. NIST. NIST арнайы басылымы 800-186: Эллиптикалық қисық криптографияға арналған нұсқаулық ; Техникалық есеп; NIST: Gaithersburg, MD, АҚШ, 2017 ж.
3. https://en.wikipedia.org/wiki/Elliptic_curve
4. Бернштейн, диджей; Lange, T. SafeCurves: Эллиптикалық-қисық криптография үшін қауіпсіз қисықтарды таңдау. 2014. Интернетте қолжетімді: **https://safecurves.cr.yp.to/** (қолжетімді 2023 жылдың 10 наурызында).
5. Рыза, Қ.; Смит, Дж.; Джонсон, А. Эллиптикалық қисықтардың қауіпсіздігі: жан-жақты зерттеу. J. Cryptogr. Аг. **2016** , 6 , 87–105
6. Гура, Н.; Пател, А.; Уандер, А.; Эберле, Х. 8-биттік процессорларда эллиптикалық қисық криптография мен RSA салыстыру. CHES **2004** , 8 , 119–132.

7. Сайто, М.; Matsumoto, M. TinyMT: Mersenne Twister шағын өлшемді нұсқасы. ACM Trans. Үлгі. Есептеу. Симул. (TOMACS) **2011** , 22 , 3

ӘОЖ 004.056.55

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ БОЙЫНША ЗЕРТТЕУ

Сооруков Даулет
dsoorukov@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Криптология кафедрасының студенті, Астана, Қазақстан
Ғылыми жетекшісі – Жетписбаев Д.

Кіріспе

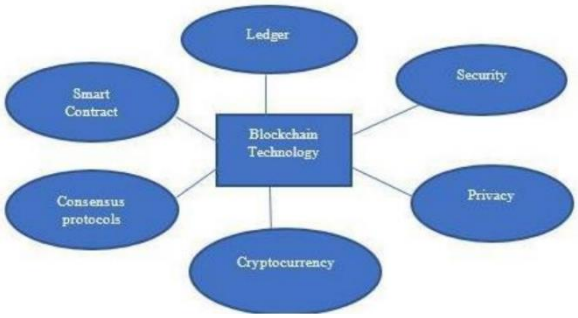
Блокчейн – орталықтандырылмаған және транзакциялық деректерді үлкен тең дәрежелі желіде ортақ пайдалануға арналған дамып келе жатқан технологиялардың бірі.
сенімсіз мүшелер бір-бірімен делдалсыз, тексерілетін түрде әрекеттесе алады. Бұл мақалада біз оның негіздерін қарастырамыз

Блокчейн, оның қолданбалары, түрлері және блокчейннің жұмысы. Бұл инновациялық техниканың артында қауіпсіздік, құпиялылық мәселелері және осы технологияның Консенсус механизмдері де маңызды және алаңдаушылық тудырады. Блокчейн технологиясымен байланысты мәселелер де осы мақалада талқыланады.

Барлық дәстүрлі транзакциялар орталықтандырылған сенімді тарапқа байланысты, бұл транзакция құнының, тиімділігінің және көптеген мәселелерін береді. Осы мәселелерді шешу және қауіпсіз, тезірек және қол жеткізу үшін мөлдір транзакциялар деген ұғымды енгізуіміз керек

Блокчейн технологиясы.

Сатоси Накамото енгізген блокчейн технологиясы. Bitcoin Blockchain қолданбаларының бірі ретінде анықталады қаржы саласындағы технология. Блокчейн - бұл бөлінген кітап технологиясы. Ол жеке тұлғалар мен ұйымдар арасындағы транзакцияларды үшінші қажетсіз өңдейді.



1-сурет: Блокчейн технологиясының жалпы архитектурасы

Блокчейн технологиялары

Блок блокчейннің бір бөлігі болып табылады, онда ол барлық ақпаратты жазады транзакциялар жасайды және ол аяқталғаннан кейін блокчейндегі тұрақты дерекқорға кіреді. Blockchain-де блоктар бір-бірімен байланыстырылған тізім сияқты. Әрбір блок хэштен тұрады