MUHANDISLIK & IQTISODIYOT

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

2026-YIL
NOYABR / 11-SON I QISM



Milliy nashrlar

OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

Google Scholar

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

OpenAIRE



ISSN: 3060-463X

РЭУ.РФ ИМЕНИ Г.В. ПЛЕХАНОВА ТАШКЕНТСКИЙ ФИЛИАЛ

TOSHKENT DAVLAT TRANSPORT UNIVERSITETI

TOSHKENT

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Elektron nashr, 2026-yil, noyabr.

Bosh muharrir:
Zokirova Nodira Kalandarovna, iqtisodiyot fanlari doktori, DSc, professor

Bosh muharrir o'rinbosari:
Shakarov Zafar G'afforovich, iqtisodiyot fanlari bo'yicha falsafa doktori, PhD, dotsent

Tahrir hay'ati:
Abduraxmanov Kalandar Xodjayevich, O'z FA akademigi, iqtisodiyot fanlari doktori, professor
Sharipov Kongratbay Avezimbetovich, texnika fanlari doktori, professor
Maxkamov Baxtiyor Shuxratovich, iqtisodiyot fanlari doktori, professor
Abduraxmanova Gulnora Kalandarovna, iqtisodiyot fanlari doktori, professor
Shaumarov Said Sanatovich, texnika fanlari doktori, professor
Turayev Bahodir Xatamovich, iqtisodiyot fanlari doktori, professor
Nasimov Dilmurod Abdulloyevich, iqtisodiyot fanlari doktori (DSc), professor
Allayeva Gulchexra Jalgasovna, iqtisodiyot fanlari doktori, professor
Arabov Nurali Uralovich, iqtisodiyot fanlari doktori, professor
Maxmudov Odiljon Xolmirzayevich, iqtisodiyot fanlari doktori, professor
Xamrayeva Sayyora Nasimovna, iqtisodiyot fanlari doktori, professor
Bobonazarova Jamila Xolmurodovna, iqtisodiyot fanlari doktori, professor
Irmatova Aziza Baxromovna, iqtisodiyot fanlari doktori, professor
Bo'taboyev Mahammadjon To'ychiyevich, iqtisodiyot fanlari doktori, professor
Shamshiyeva Nargizaxon Nosirxuja kizi, iqtisodiyot fanlari doktori, professor,
Xolmuxamedov Muhsinjon Murodullayevich, iqtisodiyot fanlari nomzodi, dotsent
Xodjayeva Nodiraxon Abdurashidovna, iqtisodiyot fanlari nomzodi, dotsent
Amanov Otabek Amankulovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent
Toxirov Jaloliddin Ochil o'g'li, texnika fanlari bo'yicha falsafa doktori (PhD)
Qurbonov Samandar Pulatovich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Zikriyoyev Aziz Sadulloyevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Tabayev Azamat Zaripbayevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Sxay Lana Aleksandrovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent
Ismoilova Gulnora Fayzullayevna, iqtisodiyot fanlari nomzodi, dotsent
Djumaniyazov Umrbek Ilxamovich, iqtisodiyot fanlari nomzodi, dotsent
Kasimova Nargiza Sabitdjanovna, iqtisodiyot fanlari nomzodi, dotsent
Kalanova Moxigul Baxritdinovna, dotsent
Ashurzoda Luiza Muxtarovna, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Sharipov Sardor Begmaxmat o'g'li, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Tursunov Ulug'bek Sativoldiyevich, iqtisodiyot fanlari doktori (DSc), dotsent
Bauyetdinov Majit Janizaqovich, Toshkent davlat iqtisodiyot universiteti dotsenti, PhD
Botirov Bozorbek Musurmon o'g'li, Texnika fanlari bo'yicha falsafa doktori (PhD)
Sultonov Shavkatjon Abdullayevich, Kimyo fanlari doktori, (DSc)
Jo'raeva Malohat Muhammadovna, filologiya fanlari doktori (DSc), professor.
Yusupov Maxamadamin Abduxamidovich, iqtisodiyot fanlari nomzodi (DSc), professor
Kalonova Moxigul Baxritdinovna, iqtisodiyot fanlari nomzodi (PhD), dotsent
Mirzayev Kulmamat Djanzakovich, iqtisodiyot fanlari nomzodi (DSc), professor.
Karimova Nilufar Sadirdin qizi, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Norboyev Odil Abrayevich, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD), dotsent
Karimova Nilufar Sadirdin qizi, iqtisodiyot fanlari bo'yicha falsafa doktori (PhD)
Pardaev Umidjon Uralovich, iqtisodiyot fanlari doktori (DSc), professor
Xolmirzayev Ulug'bek Abdulazizovich, Iqtisodiyot fanlari doktori (DSc)

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
05.01.03 – Informatikaning nazariy asoslari
05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
05.01.07 – Matematik modellashtirish
05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
05.02.00 – Mashinasozlik va mashinashunoslik
05.02.08 – Yer usti majmualari va uchish apparatlari
05.03.02 – Metrologiya va metrologiya ta'minoti
05.04.01 – Telekommunikasiya va kompyuter tizimlari, telekommunikasiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
05.05.05 – Issiqlik texnikasining nazariy asoslari
05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
05.08.03 – Temir yo'l transportini ishlatish
05.08.06 – "G'ildirakli va gusenisali mashinalar va ularni ishlatish" (texnika fanlari)
05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
08.00.01 – Iqtisodiyot nazariyasi
08.00.02 – Makroiqtisodiyot
08.00.03 – Sanoat iqtisodiyoti
08.00.04 – Qishloq xo'jaligi iqtisodiyoti
08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
08.00.06 – Ekonometrika va statistika
08.00.07 – Moliya, pul muomalasi va kredit
08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
08.00.09 – Jahon iqtisodiyoti
08.00.10 – Demografiya. Mehnat iqtisodiyoti
08.00.11 – Marketing
08.00.12 – Mintaqaviy iqtisodiyot
08.00.13 – Menejment
08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

УЛЬТРАЗВУКОВАЯ ЗАТОЧКА СПИРАЛЬНЫХ СВЕРЛ: СОВРЕМЕННОЕ СОСТОЯНИЕ ИССЛЕДОВАНИЙ И ПЕРСПЕКТИВЫ ПОВЫШЕНИЯ РАБОТОСПОСОБНОСТИ ОСЕВОГО ИНСТРУМЕНТА 9
Желтухин Андрей Владимирович
TEMIR YO‘L MASHINASOZLIGINI SANOAT KOOPERATSIYASI ASOSIDA RIVOJLANTIRISHNI BAHOLASHNING METODOLOGIK YONDASHUVLARI 16
Yuldasheva S.A
ВЛИЯНИЕ ДОЛИ АКРИЛОВОГО ВОЛОКНА НА МЕХАНИЧЕСКИЕ СВОЙСТВА ХЛОПКОВО-АКРИЛОВОЙ СМЕСОВОЙ ПРЯЖИ 22
Ражапов Одил, Нуржонов Улфат, Махкамова Шоира, Рўзибоев Нуриддин
QIŞLOQ XÖJALIGIDA IQTISODIY SAMARADORLIKNI OŞIRIŞNING USTUVOR YÖNALIŞLARI 28
Gaffarova Sarvinoz Muzaffar qizi
BARQAROR QIŞLOQ XÖJALIGINI RIVOJLANTIRIŞNING IQTISODIY MAZMUNI VA UNI BELGILOVÇI ASOSIY OMILLAR 32
Fazilov Sardor Dilmurod öğli
RENTGEN TASVIRLARINI QAYTA IŞLAŞDA QÖLLANILADIGAN TEXNOLOGIYALAR 36
Temirova Xosiyat Farxod qizi
ERKIN IQTISODIY ZONALAR SAMARADORLIGINI BAHOLAŞDA KÖP MEZONLI METODOLOGIYASI: XALQARO TAJRIBA TAHLILI VA ÖZBEKISTON UÇUN TAVSIYALAR 42
Iqboljon Zumratjonoviç Ataismatov
TUB SON NOMZODLARINI DASTLABKI FILTRLASHDA PRIMORIAL SEGMENTLAŞ STRATEGIYALARI VA GEOMETRIK PARAMETRLARNI OPTIMALLAŞTIRIŞ 48
Boyquziyev Ilhom, Jabbarov Nuriddin

TUB SON NOMZODLARINI DASTLABKI FILTRLASHDA PRIMORIAL SEGMENTLAŞ STRATEGIYALARI VA GEOMETRIK PARAMETRLARNI OPTIMALLAŞTIRIŞ

Boyquziyev Ilhom Mardanoqulovich
Muhammad al-Xorazmiy nomidagi Toşkent axborot texnologiyalari universiteti, Kiberxavfsizlik va kriminalistika kafedrasi dotsenti
E-mail: i.boyquziyev@tuit.uz

Jabbarov Nuriddin Akbarovich
Muhammad al-Xorazmiy nomidagi Toşkent axborot texnologiyalari universiteti, Kriptologiya kafedrasi assistenti
E-mail: nuriddinjabbarov2606@gmail.com

Annotatsiya. Mavjud eksperimental ma'lumotlar asosida kiçik tub bölüvçilar böyiça dastlabki filtrlash jarayonida köpaytuvçilar soni, bit uzunligi va geometrik **ösiş** asosidagi segmentlaş strategiyalari taqqoslandi. Ularning bajariliş vaqtlari mos ravişda 0,091628, 0,100015 va 0,059853 s ni taşkil etdi. Geometrik segmentlaş usuli bajariliş vaqtini mos ravişda 34,68 va 40,16 foizga qisqartirdi. Eng katta umumiy bölüvçini (greatest common divisor, GCD) hisoblaş amallarining **örtaça** soni mos ravişda 2,9163, 1,9063 va 2,2825 ni taşkil etib, amallar sonining **özi** bajariliş vaqtini belgilovçi yagona omil emasligini körsatdi. Parametrlarni alohida qidiriş jarayonida boşlanğiç hajm beşga teng bölganda eng kiçik bajariliş vaqti – 0,055368 s qayd etildi. Segmentlaş strategiyasini qöllaş natijasida dastlabki filtrni **öz** içiga olgan töliq jarayonning bajariliş vaqti 0,514 foizga qisqardi. Olingan natijalar tajribada qayd etilgan konfiguratsiyalarga tegishli bölib, ularni umumlaştiriş uçun takroriy **ölçovlar ötkaziş** talab etiladi.

Kalit sözlar: primorial segment, geometrik segmentlaş, dastlabki filtr, Miller–Rabin, operand uzunligi, erta töxtaş, parametrlarni optimallaştiriş.

Abstract. Existing experimental data were analysed to compare segmentation strategies based on the number of factors, bit length, and geometric growth in small-prime prefiltering. The corresponding execution times were 0.091628, 0.100015, and 0.059853 s, respectively. Geometric segmentation reduced execution time by 34.68% and 40.16%, respectively. The mean numbers of greatest common divisor (GCD) computations were 2.9163, 1.9063, and 2.2825, respectively, indicating that the number of operations alone is not the sole determinant of execution time. In a separate parameter search, an initial segment size of five yielded the minimum recorded execution time of 0.055368 s. The application of the segmentation strategy reduced the execution time of the complete pipeline, which already incorporated prefiltering, by 0.514%. The findings are specific to the experimentally evaluated configurations, and their generalisation requires repeated measurements.

Keywords: primorial segment, geometric segmentation, prefiltering, Miller–Rabin, operand length, early termination, parameter optimisation.

Аннотация. На основе имеющихся экспериментальных данных проведено сравнение стратегий сегментации по числу множителей, битовой длине и геометрическому росту при предварительной фильтрации по малым простым делителям. Соответствующее время выполнения составило 0,091628, 0,100015 и 0,059853 с. Применение геометрической сегментации позволило сократить время выполнения на 34,68 и 40,16% соответственно. Среднее число вычислений наибольшего общего делителя (НОД) составило 2,9163, 1,9063 и 2,2825 соответственно, что свидетельствует о том, что количество операций не является единственным фактором, определяющим время выполнения. В ходе отдельного поиска параметров минимальное зарегистрированное время выполнения, равное 0,055368 с, было достигнуто при начальном размере сегмента, равном пяти. Применение стратегии сегментации позволило сократить время выполнения полного вычислительного процесса, уже включающего предварительную фильтрацию, на 0,514%. Полученные результаты относятся к экспериментально исследованным конфигурациям, а их обобщение требует проведения повторных измерений.

Ключевые слова: **сегмент прайориала**, геометрическая сегментация, предварительная фильтрация, Миллер–Рабин, длина операнда, ранняя остановка, оптимизация параметров.

KIRIŞ

Sonlarni tublikka tekşiriş (primality testing) oldidan kiçik tub bölüvçili nomzodlarni rad etiş qimmat modulli hisoblaşlar sonini kamaytiradi. Sinov bölişlarni tub köp**a**ytuvçilar köp**a**ytmasi bilan eng katta umumiy bölüvçini (greatest common divisor, GCD) hisoblaş orqali birlaştiriş mumkin [1, 2, 3]. Uşbu tadqiqotda dastlabki filtrning (prefilter) mezonini saqlagan holda köp**a**ytuvçilarni segmentlarga taqsimlaş masalasi **örganiladi**.

Maqsad – belgilangan hajm, belgilangan bit uzunligi va geometrik segmentlaşning vaqt hamda blok yuklamasiga ta'sirini aniql**aş.** Asosiy savol: tezlikni bloklar soni, operand uzunligi va erta rad etişning qaysi birikmasi belgilaydi? Mavjud qaydlar qayta tahlil qilinib, blok statistikasi asosida qoşimça hisobiy körsatkiçlar olindi.

Segmentlar tarkibi OEIS (The On-Line Encyclopedia of Integer Sequences – butun sonlar ketma-ketliklarining onlayn ensiklopediyasi) A000040 oçiq röyxati orqali tekşirildi.[1] Unda 1000 dan kiçik 168 ta tub son mavjud. Juft nomzodlar alohida körilganda 2 çiqariladi va 3 dan 997 gaça bölgan 167 ta toq tub son qoladi. Qaydlardagi barça segment köpaytmalarining bit uzunliklari şu töplam bilan mos keldi.

MAVZUGA OID ADABIYOTLAR ŞARHI

Mahalliy tadqiqotçi Ş. B. Normatov [4] katta tub sonlarni generatsiyalaşda nomzodni dastlab kiçik tub sonlarga bölib tekşirişni tavsiya qiladi.[2] Uşbu fikr mazkur işning boşlanğiç filtrlash bosqiçiga bevosita aloqador.

O. P. Ahmedova va U. R. Mardiyev [5] ehtimollik testlarini tahlil qilib, Miller–Rabin algoritmini rekursiv funksiya orqali takomillaştiriş usulini taklif etgan.[3] Ularning maqsadi murakkab sonlarning testdan xato ötiş ehtimolini kamaytirişga qaratilgan. Bu yönalişdagi işonçlilik bahosini dastlabki filtrning tezlik bahosidan alohida körib çiqiş maqsadga muvofiq. Mazkur tadqiqotda testning içki mezoni saqlanib, undan oldingi EKUB hisoblarini taşkil etiş tartibi özgartiriladi.

U. R. Mardiyev [6] Miller–Rabin va Solovay–Strassen usullarini hisoblaş samaradorligi hamda xatolik ehtimoli böyiça qiyoslaydi.[4] Uşbu iş keyingi asosiy testni tanlaş uçun foydali.

Xorijiy olimlar G. L. Miller [1] va M. O. Rabin [2] işlari asosiy tublik tekşiruvining nazariy poydevorini taşkil etadi.[5] Solovay–Strassen [7] va Agrawal–Kayal–Saxena [8] boşqa ehtimollik va deterministik yönalişlarni ifodalaydi. Damgård, Landrock va Pomerance [9] örtaça xatolikni, Jaeschke [10] bir neçta asosdagi kuçli psevdotub sonlarni tahlil qilgan. Uşbu natijalardan kelib çiqib, filtr samaradorligi va test işonçliligi ikkita alohida mezon sifatida baholanadi.

U. M. Maurer [11] Miller–Rabin oldidagi sinov bölişning yuqori çegarasini xarajat nuqtayi nazaridan tahlil qilgan.[6] Brandt, Damgård va Landrock [12] tub sonlarni generatsiyalaşni tezlaştirişni, Brandt va Damgård [13] inkremental qidiruvni örgangan. Bu işlar dastlabki saralaşni umumiy generatsiya xarajati bilan boğlaydi.

Crandall va Pomerance [14], Cohen [15], Bach va Shallit [16] hisoblaş sonlar nazariyasini tizimli bayon qiladi. Menezes, van Oorschot va Vanstone [3] dastlabki sinov bölişni ehtimollik testidan ajratadi.[7] Uşbu manbalar segmentlaş mezonining matematik töğriligini asoslaşda qöllaniladi.

R. P. Brent va P. Zimmermann [17] köp razryadli arifmetika xarajatini operand uzunligi bilan boğlaydi.[8] Von zur Gathen va Gerhard [18] köpaytiriş, qoldiq va EKUB hisoblarining murakkabligini yoritadi. Bu yondaşuv segmentlaşdagi asosiy taqqoslaş mezonini belgilaydi: bir xil sondagi EKUB çaqiruvlari turli uzunlikdagi operandlar bilan turliça vaqt talab qilişi mumkin.

M. R. Albrecht va hammualliflar [19] noqulay kirişlarda sonlarni tublikka tekşirişning işonçliligini ta'minlaş bilan boğliq jihatlarni körsatgan.[9] Uşbu natija tezlikni oşirişda asoslar tanlovi va tekşiriş şartlarini saqlaş zarurligini asoslaydi.

T. Kalibera va R. Jones [20] vaqt ölçovlaridagi takrorlar hamda noaniqlikni baholaş usulini taklif qiladi. R. Bellman [21] esa ketma-ket qarorlarni dinamik dasturlaş bilan optimallaştiriş asoslarini bayon etadi.[10] Birinçi iş

1 OEIS Foundation. A000040, The prime numbers. https://oeis.org/A000040 Murojaat sanasi: 31.10.2026.
2 Sh. B. Normatov. Zamonaviy kriptografik algoritmlar uchun katta tub sonlarni generatsiyalash masalalari. 2016, 17–18-b. https://journal.ndpi.uz/ss/article/view/2016-3-010
3 O. P. Ahmedova, U. R. Mardiyev. A method for improving Milner-Rabin algorithm to reduce the number of false witnesses. 2023, 31–38-b. https://zienjournals.com/index.php/tjet/article/view/3636
4 U. R. Mardiyev. Analysis of Probabilistic Prime Number Generation Methods and Their Efficiency. 2025, 192–199-b. https://www.orientalpublication.com/index.php/iscrc/article/view/1870
5 G. L. Miller (1976); M. O. Rabin (1980); R. Solovay, V. Strassen (1977); M. Agrawal, N. Kayal, N. Saxena (2004); I. Damgård, P. Landrock, C. Pomerance (1993); G. Jaeschke (1993).
6 U. M. Maurer (1995); J. Brandt, I. B. Damgård, P. Landrock (1993); J. Brandt, I. B. Damgård (1993).
7 R. Crandall, C. Pomerance (2005); H. Cohen (1993); E. Bach, J. Shallit (1996); A. J. Menezes, P. C. van Oorschot, S. A. Vanstone (1996), 4-bob
8 R. P. Brent, P. Zimmermann (2010); J. von zur Gathen, J. Gerhard (2013).
9 M. R. Albrecht, J. Massimo, K. G. Paterson, J. Somorovsky (2018).
10 T. Kalibera, R. Jones (2013); R. Bellman (1952).

kiçik vaqt farqlarini ehtiyotkorlik bilan baholaşga, ikkinçisi segment çegaralarining nazariy modeliga xizmat qiladi.

TADQIQOT METODOLOGIYASI

Tadqiqotda adabiyotlar tahlili, matematik va algoritmik tahlil, qiyosiy baholaş, hisoblaş xarajatlarini modellaştiriş va parametrlar sezgirligini örganış usullari qöllaniladi. Adabiyotlar tahlili filtrlash mezoni, ehtimollik kafolati va köp razryadli arifmetika xarajatlarini ajratişga xizmat qiladi [3, 14, 17, 18]. Empirik qism mavjud qaydlarni qayta işlaşga asoslanadi.

Matematik tahlilda segmentlarning barça bölüvçilarni aynan bir martadan qamraşi va kiçik tub nomzodlarni xato rad etmaslik şartlari tekşiriladi. Algoritmik tahlil erta töxtaşning yuklamaga ta'sirini aniqlaydi. Qiyosiy usul orqali uç segmentlaş strategiyasi va boşlanğiç hajm variantlari baholanadi. Turli tajriba seriyalarining nomzodlari va vaqtlari alohida saqlanadi.

Sonli qayta hisoblaş vaqt nisbatlari, vaqt qisqarişi va EKUB çaqiruvlari sonini aniqlaş uçun qöllaniladi. Oçiq tub sonlar röyxati asosida segment çegaralari va bit uzunliklari butun sonli arifmetika bilan tekşiriladi. Xarajat modelida blokka yetiş uluşi va operand uzunligi birlaştiriladi. Dinamik dasturlaş modeli nazariy imkoniyat sifatida körib çiqiladi. Filtr va töliq jarayon samaradorligi alohida talqin qilinadi.

TAHLIL VA NATIJALAR

A. Segmentlar modeli va qarorlarning özgarmasligi

P – k ta kiçik tub sonning tartiblangan töplami. U özaro kesişmaydigan qismlarga ajratilib, har bir qismning köpaytmasi tuziladi. Primorial (primorial) – boşlanğiç ketma-ket tub sonlar köpaytmasi. Keyingi alohida blok odatda primorialning özi emas, balki ketma-ket tub sonlar guruhi köpaytmasidir

$$P = P_1 \cup \cdots \cup P_m; \quad P_i \cap P_j = \emptyset \ (i \neq j).$$

$$M_i = \prod_{p \in P_i} p; \quad M = \prod_{i=1}^{m} M_i.$$

Segmentlar ketma-ket tekşiriladi. EKUB(n, M_i) > 1 bölsa, hisoblaş erta töxtatiladi (early termination). n > max(P) şartida nomzod murakkab son hisoblanadi. Umumiy algoritmda n < 2, n = 2, n ∈ P va juft n holatlari oldindan alohida körib çiqiladi.

$$\exists i: EKUB(n, M_i) > 1 \iff \exists p \in P: p \mid n.$$

Har bir segmentning tub bölüvçilari aynan tegişli qismda joylaşadi. Har bir p faqat bitta segmentga kirgani uçun segmentlaş strategiyasini almaştiriş rad etiladigan nomzodlar töplamini saqlab qoladi. Filtrdan ötiş sonning tubligini isbotlamaydi. Keyingi Miller–Rabin bosqiçining asoslar va raundlar böyiça qoidalari özgartirilmaydi.

Birinçi strategiyada töliq bloklar 16 ta tub sondan tuziladi. Ikkinçi strategiyada köpaytma uzunligi taxminan 256 bit bilan çegaralanadi. Geometrik usulda blok hajmi ikki baravar oşadi. i indeksi noldan boşlanadi, s_0 esa boşlanğiç hajmni bildiradi. Oxirgi blok qolgan tub sonlar bilan töldiriladi:

$$s_i = min(2^i \cdot s_0, k - \sum_{j<i} s_j).$$

Strategiyalar tajribasida 10 000 nomzoddan 8394 tasi rad etilib, 1606 tasi qolgan. Parametr qidiruvida 1647 ta, töliq jarayon tajribasida esa 1618 ta nomzod qolgan. Uşbu seriyalar bitta kiriş töplami sifatida birlaştirilmaydi.

B. Blok yuklamasi va operandlar böyiça xarajat

N_i – i-blokka kirgan, R_i – unda rad etilgan nomzodlar soni. Keyingi blokka $N_{i+1} = N_i - R_i$ ta nomzod yetib boradi. Har bir kirişga bitta EKUB hisobi töğri kelsa, jami çaqiruvlar va ularning örtaça soni quyidagiça aniqlanadi:

$$Q = \sum_{i=1}^{m} N_i; \quad q = Q / N_1.$$

1-jadval

Segmentlaş vaqti va bloklar asosida hisoblangan EKUB yuklamasi

Strategiya	Bloklar	Vaqt (s)	Jami EKUB	Örtaça EKUB
16 tadan tub son	11	0,091628	29 163	2,9163

Taxminan 256 bit	6	0,100015	19 063	1,9063
Geometrik, $s_0 = 4$	6	0,059853	22 825	2,2825

Bit uzunligi böyiça segmentlaş usulida geometrik strategiyaga nisbatan 3762 ta kam EKUB hisobi bajarilgan, biroq bajariliş vaqti köproq bölgan. Uning birinçi bloki 256 bit, geometrik usulniki esa 11 bitni taşkil etgan. Har ikkala strategiyada birinçi blok barça 10 000 nomzod uçun bajariladi. Bu operand hajmining ahamiyatini körsatadi. Bloklarning bajariliş vaqti alohida ölçanmaganligi sababli umumiy farqni muayyan apparat omili bilan boğlaş uçun qöşimça ölçovlar talab etiladi [17, 18].

2-jadvalda geometrik konfiguratsiyaning yuklamasi keltirilgan. Dastlabki ikki blokda 7155 ta nomzod rad etilgan. Bu barça kirişlarning 71,55 foizini va jami rad etilgan nomzodlarning 85,24 foizini taşkil etadi.

2-jadval
Geometrik $s_0 = 4$ konfiguratsiyasida bloklar yuklamasi

Blok	Tub sonlar	Bit uzunligi	Kirişlar	Rad etilgan
1	4	11	10 000	5966
2	8	37	4034	1189
3	16	100	2845	560
4	32	244	2285	326
5	64	571	1959	257
6	43	419	1702	96

Rad etilgan nomzodlar yiğindisi 8394 tani, qolgan nomzodlar soni esa 1606 tani taşkil etadi. Boşqa ikki strategiyaning blok statistikasi ham xuddi şu yiğindiga ega. EKUB çaqiruvlari soni kirişlar ustuni yiğindisi böyiça 22 825 tani taşkil etadi.

D. Geometrik boşlanğiç hajmning sezgirligi

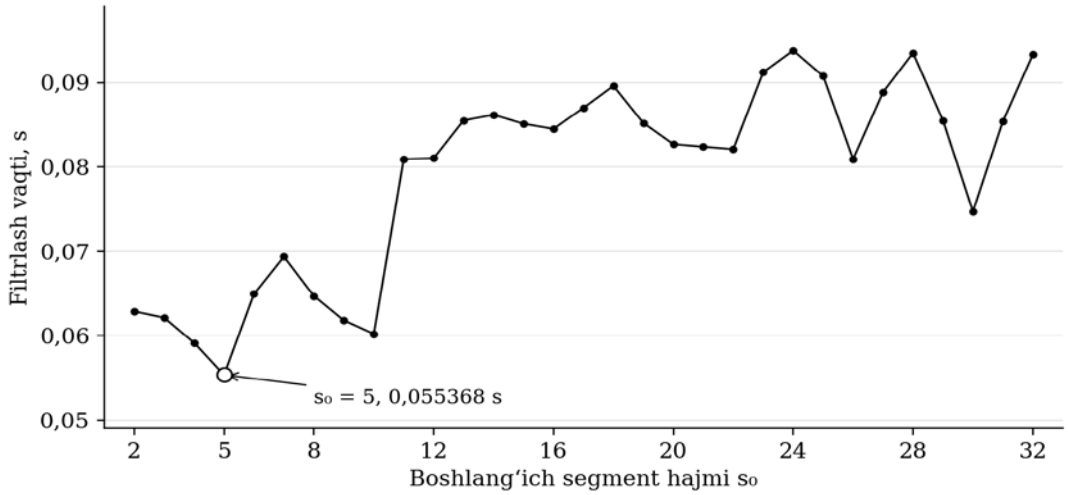
Alohida parametr tajribasida s_0 ning 2 dan 32 gaça bölgan 31 ta qiymati tekşirilgan. Barça holatlarda 1647 ta nomzod qolgan. Eng kiçik qayd etilgan vaqt $s_0 = 5$ bölganda 0,055368 s ni taşkil etgan. 3-jadvalda tanlangan qiymatlar keltirilgan.

3-jadval
Boşlanğiç hajm qidiruvidan tanlangan natijalar[11]

s_0	Bloklar	Qolganlar	Vaqt (s)
2	7	1647	0,062893
3	6	1647	0,062142
4	6	1647	0,059171
5	6	1647	0,055368
6	5	1647	0,064941
7	5	1647	0,069354
10	5	1647	0,060219
16	4	1647	0,084504
24	3	1647	0,093787
32	3	1647	0,093306

Ayni seriyadagi $s_0 = 4$ uçun 0,059171 s bazaviy qiymatga nisbatan $s_0 = 5$ bölganda bajariliş vaqti 6,43 foizga qisqargan. Oldingi strategiya tajribasidagi 0,059853 s uşbu hisobda qöllanilmagan. Bloklar sonining kamayişi bajariliş vaqtining muntazam qisqarişini ta'minlamaydi. Takroriy ölçovlar tarqoqligi böyiça ma'lumotlar mavjud bölmaganligi sababli aniqlangan minimum faqat tekşirilgan konfiguratsiyalar doirasida talqin qilinadi. Barça 31 ta qiymat 1-rasmda körsatilgan.

11 Muallif tomonidan ishlab chiqilgan



1-rasm. Boşlanğiç segment hajmi va filtrlash vaqti örtasidagi boğlaniş

$s_0 = 5$ konfiguratsiyasida blok hajmlari 5, 10, 20, 40, 80 va 12 tani, rad etilgan nomzodlar soni esa mos ravişda 6177, 1121, 476, 325, 232 va 22 tani taşkil etgan. Jami 8353 ta nomzod rad etilib, 1647 tasi qolgan. Kirişlar ketma-ketligi asosida 22 321 ta EKUB hisobi, ya'ni bir nomzodga örtaça 2,2321 ta çaqiruv töğri kelişi aniqlangan.

4-jadvalda OEIS röyxati asosida segmentlar tarkibining arifmetik tekşiruvi keltirilgan. Oraliqlardagi faqat tub sonlar köpaytirilgan. Bit uzunliklari qayta hisoblangan körsatkiçlardir.

4-jadval
Boşlanğiç hajm beş bölganda segmentlarning tub sonlar tarkibi[12]

Blok	Toq tub sonlar oraliği	Tub sonlar soni	Köpaytma bit uzunligi
1	3–13	5	14
2	17–53	10	50
3	59–151	20	133
4	157–383	40	321
5	389–911	80	744
6	919–997	12	119

Oxirgi blok qolgan 12 ta tub son bilan yakunlanadi. Dastlabki ikki blokda barça kirişlarning 72,98 foizi va jami rad etilgan nomzodlarning 87,37 foizi çiqarib taşlanadi. Bu ulüşlar ayni parametr tajribasiga tegişlidir.

E. Filtr va töliq tekşiriş jarayonini ajratiş

5-jadvalda alohida tajribadagi 1024 bitli 10 000 ta nomzod uçun umumiy bajariliş vaqti körsatilgan. Bitta primorial va segmentlangan filtr bir xil 8382 ta nomzodni rad etib, 1618 tasini Miller–Rabin testiga uzatgan.

5-jadval
Dastlabki filtrlash va segmentlaş hissasini ajratiş[13]

Usul	Umumiy vaqt (s)	Filtrsizga nisbatan S
Filtrsiz Miller–Rabin	40,763352	1,000
Bitta primorial + Miller–Rabin	10,292096	3,961
Segmentlangan filtr + Miller–Rabin	10,239206	3,981

Filtrsiz testga nisbatan 3,981 marta tezlaşiş dastlabki filtrlashning umumiy hissasini ham öz içiga oladi. Segmentlaşni bitta primorialli filtr bilan taqqoslaganda tezlaşiş 10,292096/10,239206 = 1,00517 martani, vaqt qisqarişi esa 0,514 foizni taşkil etadi. Miller–Rabin testining bajariliş vaqtiga modulli arifmetika ham ta'sir qiladi [22, 23]. Şu sababli filtr bosqiçida erişilgan vaqt tejalishini töliq jarayon samaradorligidan alohida baholaş maqsadga muvofiq.

12 OEIS A000040, n = 2…168. https://oeis.org/A000040/b000040.txt
13 Muallif tomonidan ishlab chiqilgan

Bir xil nomzodlardan iborat nazorat seriyasida filtr vaqti 0,166905 s dan 0,085654 s gaça, Miller–Rabin vaqti esa 20,473350 s dan 19,464949 s gaça özgargan. Filtr bosqiçidagi vaqt tejalishi 0,081251 s ni, umumiy farq esa 1,090192 s ni taşkil etgan. Komponentlar yiğindisi bilan umumiy vaqt örtasidagi farqni izohlaş uçun qöşimça tahlil talab etiladi. Barça usullarda 1641 ta keyingi tekşiruv va 27 ta ehtimoliy tub natija qayd etilgan. Mazkur kuzatuv umumiy vaqt farqiga segmentlaş bilan bir qatorda boşqa hisoblaş omillari ham ta'sir qilişi mumkinligini körsatadi.

OpenSSL hujjatlarida kiçik tub bölüvçilar böyiça tekşiruv va Miller–Rabin bosqiçi birgalikda tavsiflanadi. Mazkur tajribada OpenSSL qöllanilganligini aniqlaş uçun esa tegişli qaydlar talab etiladi. FIPS 186-5 standartidagi ehtimollik tekşiruvlari talablari filtrlashning vaqt natijalaridan alohida qöllaniladi. Filtrdan ötgan nomzodlar uçun asoslar tanlovi va raundlar şartlari saqlanadi.

F. Moslaşuvçan tanlaş uçun nazariy model

Geometrik ösişga qöşimça nazariy yönaliş sifatida dinamik dasturlaş modeli taklif etiladi [21]. q_i – dastlabki i ta bölüvçidan ötiş uluşi, b_{ij} – p_{i+1} dan p_j gaça bölgan köpaytmaning bit uzunligi. Xarajat faqat L va b ga boğliq bölsin. D_j dastlabki j ta bölüvçini qamrab olişning eng kiçik kutiladigan xarajatini ifodalasa, $D_0 = 0$ va $q_0 = 1$ uçun:

$$D_j = min(0 \le i < j)\{D_i + q_i \cdot G(L, b_{ij})\}.$$

Oxirgi blok i + 1 dan j gaça olinadi. k = 167 uçun 14 028 ta uzluksiz interval mavjud. Model G funksiyasini kalibrlashni talab qiladi va har bir nomzod uçun qayta yeçilmaydi. U mavjud tajribada qöllanilgan optimallaştiruvçi emas, balki keyingi tadqiqotlar uçun nazariy taklif sifatida qaraladi [17, 18, 20].

G. Parametrni tekşiriş va qayta qöllaş tartibi

Parametrni tanlaş va uni baholaş uçun alohida nomzodlar töplamlaridan foydalanış lozim. Segmentlarni tuziş, filtr va töliq jarayonning bajariliş vaqtlari alohida ölçanadi. Takroriy tajribalarda bir xil nomzodlar va asoslar ketma-ketligi saqlanadi. Takroriy ölçovlar tarqoqligini aniqlaş 0,514 foiz kabi kiçik farqlarning barqarorligini baholaş imkonini beradi [20].

Python hujjatlarida keltirilgan perf_counter va perf_counter_ns funksiyalari ötgan vaqtni ölçaşga xizmat qiladi. Natijaning nanosekundlarda ifodalanişi ölçovning haqiqiy aniqligi bir nanosekundga teng ekanligini anglatmaydi.

XULOSA VA TAKLIFLAR

Bir xil tub bölüvçilar töplamida segmentlaş filtr qarorining özgarmasligini saqlagan holda operand hajmlari va blok yuklamasini özgartiradi. Geometrik segmentlaş strategiyasi belgilangan hajmga asoslangan usulga nisbatan bajariliş vaqtini 34,68 foizga, bit uzunligi böyiça segmentlaş usuliga nisbatan esa 40,16 foizga qisqartirgan. Olingan natijalar hisoblaş samaradorligini baholaşda EKUB çaqiruvlari soni bilan bir qatorda operandlarning bit uzunligi va ular bilan boğliq arifmetik xarajatlarni ham hisobga oliş zarurligini körsatadi.

Parametr qidiruvi natijasida $s_0 = 5$ konfiguratsiyasida eng kiçik bajariliş vaqti – 0,055368 s qayd etilgan. Mazkur natija tekşirilgan hisoblaş muhiti va eksperimental konfiguratsiyalarga tegişli. Dastlabki filtrni öz içiga olgan töliq tekşiriş jarayonida segmentlaşning qöşimça samaradorligi 0,514 foizni taşkil etgan. Bu esa segmentlaş strategiyasining samaradorligini filtr bosqiçi va töliq hisoblaş jarayoni kesimida alohida baholaş muhimligini tasdiqlaydi.

Olingan natijalardan kelib çiqib, quyidagi takliflar ilgari suriladi:

1. Geometrik segmentlaş parametrlarini optimallaştiriş. Tub son nomzodlarini dastlabki filtrlashda geometrik segmentlaş strategiyasidan foydalanış, boşlanğiç segment hajmini esa nomzodlarning bit uzunligi, bloklar soni va operand hajmini hisobga olgan holda tanlaş taklif etiladi. Xususan, tajribada samarali natija körsatgan $s_0 = 5$ konfiguratsiyasini keyingi qiyosiy sinovlar uçun tayanç variant sifatida qöllaş maqsadga muvofiq.

2. Hisoblaş xarajatlarini kompleks baholaş tizimini takomillaştiriş. Segmentlaş strategiyalarining samaradorligini aniqlaşda EKUB çaqiruvlari soni, operandlarning bit uzunligi, bloklarga yetib boriş uluşi va bajariliş vaqtini birgalikda hisobga oluvçi xarajat modelidan foydalanış tavsiya etiladi. Bu yondaşuv segment çegaralarini asosli tanlaş hamda dinamik dasturlaş asosida moslaşuvçan optimallaştiriş algoritmlarini işlab çiqiş uçun nazariy asos yaratadi.

3. Eksperimental natijalarning barqarorligini tekşiriş va amaliy qöllaş imkoniyatlarini kengaytiriş. Tanlangan segmentlaş konfiguratsiyalarini turli bit uzunliklariga ega nomzodlar töplamlarida, bir xil hisoblaş şertlari asosida takroriy sinovlardan ötkaziş taklif etiladi. Bunda filtr va töliq tekşiriş jarayonlarining bajariliş vaqtlarini alohida qayd etiş, ölçovlar tarqoqligini baholaş hamda parametr tanlovining barqarorligini aniqlaş maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR RÖYXATI

1. Miller G. L. Riemann's Hypothesis and Tests for Primality // Journal of Computer and System Sciences. – 1976. – Vol. 13, No. 3. – P. 300–317. – DOI: 10.1016/S0022-0000(76)80043-8.
2. Rabin M. O. Probabilistic Algorithm for Testing Primality // Journal of Number Theory. – 1980. – Vol. 12, No. 1. – P.

128–138. – DOI: 10.1016/0022-314X(80)90084-0.
3. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – Boca Raton: CRC Press, 1996. – Ch. 4. – URL: https://cacr.uwaterloo.ca/hac/about/chap4.pdf.
4. Normatov Sh. B. Zamonaviy kriptografik algoritmlar uchun katta tub sonlarni generatsiyalash masalalari // Ilim hám jámiyet (Science and Society). – 2016. – No. 3. – B. 17–18. – URL: https://journal.ndpi.uz/ss/article/view/2016-3-010.
5. Ahmedova O. P., Mardiyev U. R. A Method for Improving Milner-Rabin Algorithm to Reduce the Number of False Witnesses // Texas Journal of Engineering and Technology. – 2023. – Vol. 18. – P. 31–38. – URL: https://zienjournals.com/index.php/tjet/article/view/3636.
6. Mardiyev U. R. Analysis of Probabilistic Prime Number Generation Methods and Their Efficiency // International Scientific and Current Research Conferences. – 2025. – Vol. 1, No. 01. – P. 192–199. – URL: https://www.orientalpublication.com/index.php/iscrc/article/view/1870.
7. Solovay R., Strassen V. A Fast Monte-Carlo Test for Primality // SIAM Journal on Computing. – 1977. – Vol. 6, No. 1. – P. 84–85. – DOI: 10.1137/0206006.
8. Agrawal M., Kayal N., Saxena N. PRIMES Is in P // Annals of Mathematics. – 2004. – Vol. 160, No. 2. – P. 781–793. – URL: https://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf.
9. Damgård I., Landrock P., Pomerance C. Average Case Error Estimates for the Strong Probable Prime Test // Mathematics of Computation. – 1993. – Vol. 61, No. 203. – P. 177–194. – DOI: 10.1090/S0025-5718-1993-1189518-9.
10. Jaeschke G. On Strong Pseudoprimes to Several Bases // Mathematics of Computation. – 1993. – Vol. 61, No. 204. – P. 915–926. – DOI: 10.1090/S0025-5718-1993-1192971-8.
11. Maurer U. M. Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters // Journal of Cryptology. – 1995. – Vol. 8, No. 3. – P. 123–155. – URL: https://crypto.ethz.ch/publications/Maurer95a.html.
12. Brandt J., Damgård I. B., Landrock P. Speeding Up Prime Number Generation // Advances in Cryptology – ASIACRYPT '91. Lecture Notes in Computer Science. – Berlin: Springer, 1993. – Vol. 739. – P. 440–449. – URL: https://pure.au.dk/portal/en/publications/speeding-up-prime-number-generation/.
13. Brandt J., Damgård I. B. On Generation of Probable Primes by Incremental Search // Advances in Cryptology – CRYPTO '92. Lecture Notes in Computer Science. – Berlin: Springer, 1993. – Vol. 740. – P. 358–370. – URL: https://pure.au.dk/portal/en/publications/on-generation-of-probable-primes-by-incremental-search.
14. Crandall R., Pomerance C. Prime Numbers: A Computational Perspective. – 2nd ed. – New York: Springer, 2005. – DOI: 10.1007/0-387-28979-8.
15. Cohen H. A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics. – Berlin: Springer, 1993. – Vol. 138. – DOI: 10.1007/978-3-662-02945-9.
16. Bach E., Shallit J. Algorithmic Number Theory. Vol. 1: Efficient Algorithms. – Cambridge, MA: MIT Press, 1996. – URL: https://cs.uwaterloo.ca/~shallit/ant.html.
17. Brent R. P., Zimmermann P. Modern Computer Arithmetic. – Cambridge: Cambridge University Press, 2010. – DOI: 10.1017/CBO9780511921698.
18. von zur Gathen J., Gerhard J. Modern Computer Algebra. – 3rd ed. – Cambridge: Cambridge University Press, 2013. – DOI: 10.1017/CBO9781139856065.
19. Albrecht M. R., Massimo J., Paterson K. G., Somorovsky J. Prime and Prejudice: Primality Testing Under Adversarial Conditions // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018. – P. 281–298. – DOI: 10.1145/3243734.3243787.
20. Kalibera T., Jones R. Rigorous Benchmarking in Reasonable Time // Proceedings of the 2013 International Symposium on Memory Management. – 2013. – P. 63–74. – URL: https://kar.kent.ac.uk/33611/.
21. Bellman R. On the Theory of Dynamic Programming // Proceedings of the National Academy of Sciences of the United States of America. – 1952. – Vol. 38, No. 8. – P. 716–719. – DOI: 10.1073/pnas.38.8.716.
22. Montgomery P. L. Modular Multiplication without Trial Division // Mathematics of Computation. – 1985. – Vol. 44, No. 170. – P. 519–521. – DOI: 10.1090/S0025-5718-1985-0777282-X.
23. Koç Ç. K., Acar T., Kaliski B. S. Jr. Analyzing and Comparing Montgomery Multiplication Algorithms // IEEE Micro. – 1996. – Vol. 16, No. 3. – P. 26–33. – DOI: 10.1109/40.502403.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Abdurahmon Qurbonov

2026. № 11

© Materiallar ko'chirib bosilganda "Muhandislik va iqtisodiyot" jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

**Manzilimiz: Toshkent shahri Yunusobod
tumani 15-mavze 19-uy**


+998 93 718 40 07

https://muhandislik-iqtisodiyot.uz/index.php/journal

t.me/yait_2100