

MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI
FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

“AL-FARG‘ONIIY AVLODLARI”

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI



4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON



O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
FARG'ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali.

Chop etish tili: O'zbek, ingliz, rus. Jurnal texnika fanlariga ixtisoslashgan bo'lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo'nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.

Язык издания: узбекский, английский, русский. Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.

Language of publication: Uzbek, English, Russian. The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №4
Vol.1, Iss.4, 2023 y

ELEKTRON ILMIY JURNALI

ELECTRONIC SCIENTIFIC JOURNAL

«Al-Farg'oniyl avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») O'zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro'yxatdan o'tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo'nalishida milliy nashrlar ro'yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg'ona sh.,
Aeroport ko'chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2023 YIL

TAHRIR HAY'ATI

Maxkamov Baxtiyor Shuxratovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

Muxtarov Farrux Muhammadovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

Arjannikov Andrey Vasilevich,

Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

Satibayev Abdugani Djunosovich,

Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

Rasulov Akbarali Maxamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

Yakubov Maksadxon Sultaniyazovich,

Muhammad al-Xorazmiy nomidagi TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

G'ulomov Sherzod Rajaboyevich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

G'aniyev Abduxalil Abdjalilovich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

Zaynidinov Hakimjon Nasritdinovich,

Muhammad al-Xorazmiy nomidagi TATU Kompyuter injiniringi fakulteti, Sun'iy intellekt kafedrasida texnika fanlari doktori, professor

Bo'taboyev Muhammadjon To'ychiyevich,

Farg'ona politexnika instituti, Iqtisod fanlari doktori, professor

Abdullayev Abdujabbor,

Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

Qo'ldashev Abbosjon Hakimovich,

O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

Ergashev Sirojiddin Fayazovich,

Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

Qoraboyev Muhammadjon Qoraboevich,

Toshkent tibbiyot akademiyasi Farg'ona filiali fizika matematika fanlari doktori, professor, BMT ning maslahatchisi maqomidagi xalqaro axborotlashtirish akademiyasi akademigi

Polvonov Baxtiyor Zaylobiddinovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

Zulunov Ravshanbek Mamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Dasturiy injiniring kafedrasida dotsenti, fizika-matematika fanlari nomzodi

Saliyev Nabijon,

O'zbekiston jismoniy tarbiya va sport universiteti Farg'ona filiali dotsenti

Abdullaev Temurbek Marufovich,

Muhammad al-Xorazmiy nomidagi TATU Axborot texnologiyalari kafedra mudiri, texnika fanlar bo'yicha falsafa doktori

Zokirov Sanjar Ikromjon o'g'li,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Muxtarov Farrux Muhammadovich, TARMOQ TRAFIGI ANOMALIYALARINI IDENTIFIKATSIYA QILISHNING STATIK USULI	4-7
Daliyev Baxtiyor Sirojiddinovich, Abelning umumlashgan integral tenglamasini yechish uchun Sobolev fazosida optimal kvadratur formulalar	8-14
Umarov Shuxratjon Azizjonovich, KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI	15-21
Zulunov Ravshanbek Mamatovich, PYTHONDA NEYRON TARMOQNI QURISH VA BASHORAT QILISH	22-26
Djalilov Mamatisa Latibdjanovich, IKKI QATLAMLI NOELASTIK PLASTINKANING KO'NDALANG TEBRANISHI UMUMIY TENGLAMASINI TAHLIL QILISH	27-30
Erkin Uljaev, Azizjon Abdulkhamidov, Utkirjon Ubaydullayev, A Convolutional Neural Network For Classification Cotton Boll Opening Degree	31-36
Seytov Aybek Jumabayevich, Xusanov Azimjon Mamadaliyevich, Magistral kanallarda suv resurslarini boshqarish jarayonlarini modellashtirish algoritmini ishlab chiqish	37-43
Abdullayev Temurbek Marufjonovich, Algorithm of functioning of intellectual information-measuring system	44-49
Odinakhon Sadikovna Rayimjanova, Usmonali Umarovich Iskandarov, Reaserch of highly sensitive deformation semiconductor sensors based on AFV	50-53
S.S.Radjabov, G.R.Mirzayeva, A.O.Tillavoldiyev, J.A.Allayorov, BARG TASVIRI BO'YICHA MADANIY O'SIMLIK LARNING FITOSANITAR HOLATINI ANIQLASH ALGORITMLARI	54-59
Эргашев Отабек Мирзапулатович, Интеллектуальный оптоэлектронный прибор для учета и контроля расходом воды в открытых каналах	60-65
Xomidov Xushnudbek Rapiqjon o'g'li, Nurmatov Sardorbek Xasanboy o'g'li, Yo'ldashev Bilol Iqboljon o'g'li, O'lmasov Farrux Yorqinjon o'g'li, Konus setkali chang tozalovchi qurilma uchun chang namunalarning dispers tarkibi tahlili	66-69
Akhundjanov Umidjon Yunus ugli, VERIFICATION OF STATIC SIGNATURE USING CONVOLUTIONAL NEURAL NETWORK	70-74
Лазарева Марина Викторовна, Горовик Александр Альфредович, Цифровизация и цифровой менеджмент в современном управлении	75-81
D.X.Tojimatov, KIBERTAHDIDLARNI OLDINI OLIHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI	82-85
Muxtarov Farrux Muhammadovich, Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, Kompyuter eksperimenti orqali kam atomli mis klasterlarining geometrik tuzilishini o'rganish	86-89
Umurzakova Dilnoza Maxamadjanovna, BOSHQARISH QONUNLARINI ADAPTATSIYALASH ALGORITMLARINI ISHLAB CHIQLASH	90-94
Muxamedieva Dildora Kabilovna, Muxtarov Farrux Muhammadovich, Sotvoldiev Dilshodbek Marifjonovich, JAMOAT TRANSPORTI MARSHRUTLARINI QURISH INTELLEKTUAL ALGORITMLARI	95-103
Нурдинова Разияхон Абдихаликовна, Перспективы применения элементов с аномальными фотовольтаическими напряжениями	104-108
Bozarov Baxromjon Pخomovich, UCH O'LCHOVLI FAZODAGI SFERADAANIQLANGAN FUNKSIYALARNI TAQRIBIY INTEGRALLASH UCHUN OPTIMAL KUBATUR FORMULALAR	109-113
Улжаев Эркин, Худойбердиев Элёр Фахриддин угли, Нарзуллаев Шохрух Нурали угли, РАЗРАБОТКА КОНСТРУКЦИИ И ФУНКЦИОНАЛЬНОЙ СХЕМЫ ПОЛУЦИЛИНДРИЧЕСКОГО ЁМКОСТНОГО ПОТОЧНОГО ВЛАГОМЕРА	114-122
Mamirov Uktam Farkhodovich, Buronov Bunyod Mamurjon ugli, ALGORITHMS FOR FORMATION OF CONTROL EFFECTS IN CONDITIONS OF UNOBSERVABLE DISTURBANCES	123-127
Sharibayev Nosirjon Yusubjanovich, Jabborov Anvar Mansurjonovich, YURAK-QON TOMIR KASALLIKLARI DIAGNOSTIKASI UCHUN TEXNOLOGIYALAR, ALGORITMLAR VA VOSITALAR	128-136
Marina Lazareva, Estimating development time and complexity of programs	137-141
Asrayev Muhammadmullo, ONLINE HANDWRITING RECOGNITION	142-146
Norinov Muhammadyunus Usibjonovich, SPEKTR ZONALI TASVIRLARGA INTELLEKTUAL ISHLOV BERISH USULLARI TAHLILI	147-152
Xudoynazarov Umidjon Umarjon o'g'li, PARAMETRLI ALGEBRAGA ASOSLANGAN EL-GAMAL SHIFRLASH ALGORITMLARINI GOMOMORFIK XUSUSIYATINI TADQIQ ETISH	153-157
D.M.Okhunov, M.Okhunov, THE ERA OF THE DIGITAL ECONOMY IS AN ERA OF NEW OPPORTUNITIES AND PROSPECTS FOR BUSINESS DEVELOPMENT BASED ON CROWDSOURCING TECHNOLOGIES	158-165

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Солиев Бахромжон Набиджонович, Путеводитель по построению веб-API на Django - Шаг за шагом с Django REST framework — от моделей до проверки работоспособности	166-171
Sevinov Jasur Usmonovich, Boborayimov Okhunjon Khushmurod ogli, ALGORITHMS FOR SYNTHESIS OF ADAPTIVE CONTROL SYSTEMS WITH IMPLICIT REFERENCE MODELS BASED ON THE SPEED GRADIENT METHOD	172-176
Mamatov Narzullo Solidjonovich, Jalelova Malika Moyatdin qizi, Tojiboyeva Shaxzoda Xoldorjon qizi, Samijonov Boymirzo Narzullo o'g'li, SUN'IY YO'LDOSHDAN OLINGAN TASVIRDAGI DALA MAYDONI CHEGARALARINI ANIQLASH USULLARI	177-181
Обухов Вадим Анатольевич, Криптография на основе эллиптических кривых (ECC)	182-188
Turdimatov Mamirjon Mirzayevich, Sadirova Xursanoy Xusanboy qizi, AXBOROTNI HIMOYALASHDA CHETLAB O'TISHNING MUMKIN BO'LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI	189-193
Musayev Xurshid Sharifjonovich, TRIKOTAJ MAHSULOTLARIDA NUQSONLI TO'QIMALARNING ANIQLASHNING MATEMATIK MODELI VA UNING ALGORITMLARI	194-196
Kodirov Ahkhmadkhon, Umarov Abdumukhtar, Rozaliyev Abdumalikjon, ANALYSIS OF FACIAL RECOGNITION ALGORITHMS IN THE PYTHON PROGRAMMING LANGUAGE	197-205
Suyumov Jorabek Yunusalievich, METHODOLOGICAL PROBLEMS OF QUALIMETRY IN CONDUCT OF PEDAGOGICAL EXPERIMENT-EXAMINATION	206-211
Хаджаев Саидакбар Исмоил угли, АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОТ КИБЕРАТАК	212-217
M.M.Khalilov, Effect of Heat Treatment on the Photosensitivity of Polycrystalline PbTe Films AND PbS	218-221
Тажибаев Илхом Бахтиёрвич, ПОЛНОСТЬЮ ВОЛОКОННЫЙ СЕНСОР, ОСНОВАННЫЙ НА КОНСТРУКЦИИ ИЗ МАЛОМОДОВОГО ВОЛОКОННОГО СМЕЩЕНИЯ С КАСКАДНЫМ СОЕДИНЕНИЕМ ВОЛОКОННОЙ РЕШЕТКИ С БОЛЬШИМ ИНТЕРВАЛОМ, ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ИСКРИВЛЕНИЯ И ПРОВЕДЕНИЯ АКУСТИЧЕСКИХ ИЗМЕРЕНИЙ	222-225
Sharibaev Nosir Yusubjanovich, Djuraev Sherzod Sobirjanovich, To'xtasinov Davronbek Xoshimjon o'g'li, PRIORITIES IN DETERMINING ELECTRIC MOTOR VIBRATION WITH ADXL345 ACCELEROMETER SENSOR	226-230
Mukhammadjonov A.G., ANALYSIS OF AUTOMATION THROUGH SENSORS OF HEAT AND HUMIDITY OF DIFFERENT DIRECTIONS	231-236
Эрматова Зарина Кахрамоновна, АКТУАЛЬНОСТЬ ПРЕПОДАВАНИЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ C++ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ	237-241
Saparbaev Rakhmon, ANALOG TO DIGITAL CONVERSION PROCESS BY MATLAB SIMULINK	242-245
Садикова М.А., Авазова Н.К., САМООБУЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, БАЗОВЫЕ ПРИНЦИПЫ РАБОТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРОСТОМ ПРИМЕРЕ	246-250
Abduhafizov Tohirjon Ubaydullo o'g'li, Abdurasulova Dilnoza Botirali kizi, DEVELOPMENT OF ALGORITHMS IN THE ANALYSIS OF DEMAND AND SUPPLY PROCESSES IN ECONOMIC SYSTEMS	251-256
Kayumov Ahror Muminjonovich, CREATING MATHEMATICAL MODELS TO IDENTIFY DEFECTS IN TEXTILE MACHINERY FABRIC	257-261
Mirzakarimov Baxtiyor Abdusalomovich, Xayitov Azizjon Mo'minjon o'g'li, BIOMETRIC METHODS SECURE COMPUTER DATA FROM UNAUTHORIZED ACCESS	262-266
Soliyev B., Odilov A., Abdurasulova Sh., Leveraging Python for Enhanced Excel Functionality: A Practical Exploration	267-271
Жураев Нурмахамад Маматович, Системы Электроснабжения Оборудования Предприятий Связи: Надежность и Эффективность	272-276
Rasulova Feruzaxon Xoshimjon qizi, Isroilov Sharobiddin Mahammadyusufovich, OLIY TA'LIM MUASSASALARIDA MUTAXASSISILIK FANLARINI O'QITISHDA MULTIMEDIALI MOBIL ILOVADANDAN FOYDALANISHNING STATISTIK TAHLILI	277-280
Muxtarov Farrux Muxammadovich, Toshpulatov Sherali Muxamadaliyevich, SUN'IY INTELLEKT YORDAMIDA IJTIMOYIY TARMOQ MONITORINGI TIZIMINI YARATISH, AFZALLIKLARI VA MUHIM JIXATLARI	281-285
Sadikova Munira Alisherovna, APPLICATION OF ARTIFICIAL INTELLIGENCE DEVICES IN MANUFACTURING	286-290
Mamatov Narzullo Solidjonovich, Ibroximov Sanjar Rustam o'g'li, Fayziyev Voxid Orzumurod o'g'li, Samijonov Abdurashid Narzullo o'g'li, SUN'IY INTELLEKT VOSITALARINI TA'LIMNI NAZORAT QILISH VA BAHOLASHDA QO'LLASH	291-297

PARAMETRLI ALGEBRAGA ASOSLANGAN EL-GAMAL SHIFRLASH ALGORITMLARINI GOMOMORFIK XUSUSIYATINI TADQIQ ETISH

Xudoynazarov Umidjon Umarjon o‘g‘li,
Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti Farg‘ona filiali, “Axborot xavfsizligi”
kafedrasida katta o‘qituvchisi
umidjonxudoynazarov@gmail.com

Annotatsiya: Gomomorfik shifrlash algoritmlari shifrlangan ma’lumotlar ustida ularni deshifrlamasdan amallar bajarish imkoniyatini beradi. Bu esa axborotni konfidensialligini ta’minlaydi. El-Gamal gomomorfik shifrlash algoritmi bo‘lib, u diskret logarifmlash muammosiga asoslangan. Hozirda mavjud assimmetrik shifrlash algoritmlari bir tomonlama funksiyalarga asoslangan chekli maydonda diskret logarifmlash, faktorlash va daraja parametri kabi murakkabliklarga asoslangan. Maqolada yetarlicha katta chekli maydonda diskret logarifmlash amaliga teng kuchli bo‘lgan, bir tomonlama funksiyaga asoslangan parametrli shifrlash algoritmlarining gomomorfik xususiyatlari tadqiq etilgan.

Kalit so‘zlar: Kriptografiya, El-Gamal algoritmi, kriptobardoshlilik, bir tomonlama funksiya, diskret logarifmlash, faktorlash, teskarilash, elliptik egri chiziqlar, Gomomorfik shifrlash

Kirish. Bugungi kunda bulutli hisoblash tizimi axborot texnologiyalari sohasining muhim yo‘nalishlariga aylanmoqda. Bulutli hisoblash tizimi bir qator apparat va dasturiy ta’minot manbalariga Internet orqali ulanib foydalanish imkoniyatini taqdim etadi. Bulutli hisoblash tizimining tez suratlarda rivojlanishi axborotlarni konfidensiallik, butunlik hamda foydalanuvchanlik bilan bog‘liq turli xil axborot xavfsizligi muammolarini keltirib chiqarmoqda. An’anaviy shifrlash texnologiyasi ma’lumotlarni saqlashda va uzatilishida axborot xavfsizligini ta’minlaydi, lekin axborotga ishlov berishda samarasiz hisoblanadi. Axborotni bulutli tizimlarda shifrlangan holda saqlash uchun bulutga yuklangan har bir faylni kriptografik vosita orqali shifrlashdan kerak. Bulutli tizimdagi ma’lumotlarni faqat maxfiy kalit egasidan boshqa hech kim olmaydi. Ushbu usul jismoniy shaxslar yoki kichik tashkilotlar uchun juda mos keladi. Gomomorfik kriptografik algoritmlar esa, bulutli tizimlarda axborotlarga xavfsiz ishlov berish imkonini beradi.

Ushbu maqolada parametrli algebra asosida takomillashtirilgan El-Gamal ochiq kalitli kriptografik algoritmining gomomorfik xususiyatlarini ko‘rib chiqamiz.

Adabiyotlar tahlili va metodologiya.

Maqolada hozirgi kunda axborot xavfsizligini

ta’minlash usullari va vositalari yoritilgan adabiyotlar o‘rganib chiqildi. Shu jumladan G‘aniyev S.K., Tashev K.A., “Axborot xavfsizligi”, X.P Xasanovning “Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari”, Akbarov D.E “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” adabiyotlari o‘rganib chiqildi. Shu bilan birga Фороузан .Б.А. «криптография и безопасность сетей» va bir qancha kriptografiyaga oid xorijiy adabiyotlar, ilmiy maqolalar va ro‘znomalar tadqiq qilindi.

Gomomorfik shifrlash algoritmlari. Shaxsiy va ochiq kalitlarni shifrlashdan ko‘ra ancha kuchli va xavfsiz shifrlash bu gomomorf shifrlashdir. Gomomorf shifrlash - bu ochiq matnni shifrlash va shifrlangan matn bo‘yicha hisoblashlarni ochiq matnni oshkor qilmasdan, ya’ni uni parolini ochmasdan amalga oshirish usuli hisoblanadi[6].

Gomomorf shifrlashning ta’rifida aytilganidek, boshqa shifrlashlardan farqli o‘laroq, gomomorf shifrlash shifrlangan matnlarda amalga oshiriladigan hisob-kitoblarni o‘z ichiga oladi, ochiq matnda emas. Shifrlangan ma’lumotlarni hisoblash shuni anglatadiki, agar foydalanuvchi F funksiyaga ega bo‘lsa, va qandaydir m_1, m_2, \dots, m_n kiruvchilar uchun $f(m_1, m_2, \dots, m_n)$ natijani olmoqchi bo‘lsa,



uning o'rniga c_1, c_2, \dots, c_n kiruvchi shifratni qiymatlarini hisoblash, $f(m_1, m_2, \dots, m_n)$ qiymatni deshifrlagandagidek natijani olish imkoniga ega bo'ladi. HE ning bu xususiyati uni boshqa shifrlash algoritmlariga qaraganda mustahkamroq va xavfsizroq qiladi.

Gomomorfik shifrlashning uchta asosiy turi mavjud. Ularning orasidagi asosiy farq shifrlash matnida bajarilishi mumkin bo'lgan matematik operatsiyalarning turlari va chastotalariga bog'liq. Gomomorfik shifrlashning uch turi bor:

- Qisman (Partially) gomomorfik shifrlash
- Qisman (Somewhat) gomomorfik shifrlash
- To'liq (Fully) gomomorfik shifrlash.

Qisman gomomorfik shifrlash (PHE) maxfiy ma'lumotlarni saqlashga yordam beradi, bu faqat tanlangan matematik funksiyalarni shifrlangan qiymatlarda bajarishga imkon beradi. Bu shuni anglatadiki, bitta operatsiya shifrlash matnida cheksiz ko'p marta bajarilishi mumkin. Qisman gomomorfik shifrlash SSL / TLS orqali xavfsiz ulanishni o'rnatishda keng qo'llaniladigan RSA shifrlash uchun asosdir. PHE-ning ba'zi misollariga ElGamal shifrlash (multiplikativ sxema) va Pailliyer(Qo'shish sxemasi) shifrlash kiradi.

To'liq bo'lmagan shifrlash (SHE) sxemasi ma'lum bir murakkablikgacha cheklangan operatsiyalarni qo'llab-quvvatlaydigan (masalan, qo'shish yoki ko'paytirish), ammo bu operatsiyalar faqat bir necha marta bajarilishi mumkin. Bu to'liq gomomorfik shifrlash uchun asos bo'lib, uni quyida batafsil ko'rib chiqamiz.

To'liq gomomorfik shifrlash (FHE), ishlab chiqilayotgan paytda, maxfiylikni saqlash va ma'lumotni saqlashga va shu bilan birga kirishga yordam beradigan funktsional imkoniyatlarga mos kelish uchun katta imkoniyatlarga ega. Biroz gomomorfik shifrlash sxemasidan kelib chiqqan holda, ushbu muqaddas kriptografiya har qanday samarali hisoblanadigan funksiyalarni necha marotaba ishlatishga qodir va ko'p partiyali hisoblashlarni yanada samaraliroq qiladi. Gomomorfik shifrlashning boshqa shakllaridan farqli o'laroq, u shifrlangan matnlaringizda o'zboshimchalik bilan hisob-kitoblarni amalga oshirishi mumkin.

Materiallar va usullar: Ma'lumki El-Gamal qisman gomomorfik shifrlash (Partially Homomorphic Encryption (PHE)) turlariga mansub. Ushbu algoritmlar yordamida faqat ko'paytirish bilan bog'liq gomomorfik amallarni bajarishimiz mumkin.

Dastlab El-Gamal algoritmlarini gomomorfik xususiyatlarini ko'rib chiqamiz:

El-Gamal algoritmidagi siklik guruh G uning tartibi q va asos g bo'lganda, ochiq kalit (G, q, g, y) ga teng. Bu yerd, $y = g^x \pmod q$ va x esa maxfiy kalit. Bu holda ma'lumotni shifrlash funksiyasi $r \in \{0, \dots, q-1\}$ lar uchun $\varepsilon(m) = (g^r, m \cdot h^r)$ ga teng. Ushbu algoritm uchun gomomorfik xususiyat quyidagi teng bo'ladi.

$$\begin{aligned} \varepsilon(m_1) \cdot \varepsilon(m_2) &= (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) \\ &= ((g^{r_1+r_2}, (m_1 \cdot m_2)h^{r_1+r_2}) \\ &= \varepsilon(x_1 x_2) \end{aligned}$$

El-Gamal algoritmining kriptobardoshlilik chekli maydonda diskret logarifmlash muammosiga asoslanadi. Agar $\{q, a, y\}$ qiymatlarni bilgan holda, q ning yetarlicha katta miqdorida x maxfiy kalitning qiymatini $x = \log_a y$ ifoda bilan hisoblashning amalda iloji yo'q yoki bu juda katta resurs va vaqt talab qiladi.

Bugungi kunda soniyasiga juda ko'plab amallarni bajaradigan superkompyuterlar juda ham katta resursga ega bo'lib, yuqoridagi bardoshlilikni ta'minlash uchun kalit uzunligini keskin oshirishga to'g'ri keladi. Bu esa, kriptotizimning kalitlarni hosil qilish, shifrlash va deshifrlash jarayonlarini sekinlashtiradi.

Yuqoridagi xulosani inobatga olgan holda, butun sonlarni parametrlilik ko'paytirish, teskarilash va darajaga oshirish amallaridan foydalanilgan holda El-Gamal kriptotizimlarini takomillashtirish usullari taklif etilgan.

Parametrlilik algebra. Ko'p hollarda mavjud kriptografik algoritmlar parametrlilik algebrasi asosida yaratilgan algoritmlarning hususiy holi bo'lib qolmoqda.

Parametrlilik algebrasida asosiy amallar quyidagicha aniqlanadi:

1) Parametr R li ko'paytirish amali

$$a \otimes b \equiv a + b + a * R * b \pmod n$$

parametrlilik algebrasida koeffitsiyent yoki parametr deb atalishi mumkin. $R = 0$ bo'lganda bu ifoda klassik algebradagi qo'shish amali ifodalaydi.



2) Modul n bo'yicha parameter R li teskarilash amali $a^{-1} \equiv a * (1 + R * a)^{-1} \pmod{n}$, bu yerda -1 modul n bo'yicha teskarilash amali, -1 esa parametr R va modul n bo'yicha teskarilash amali bo'lib $a \otimes a^{-1} \equiv 0 \pmod{n}$ taqqoslamani qanoatlantiradi.

Parametrlar algebrasida 0 birlik elementi hisoblanib, $a \otimes 0 \equiv a \pmod{n}$ xossaga ega.

3) Parametr R li darajaga oshirish amali

$$a^{x+1} \equiv a * \sum_{i=0}^{i=x} F^i \pmod{n}, \text{ bunda } F = 1 + R * a.$$

a^{37} darajasini hisoblash uchun:

$$a^{37} \equiv a^{32+4+1} =$$

$$\left(\left(\left(\left(\left((a^2)^2 \right)^2 \right)^2 \right)^2 \right)^2 \right)^2 \otimes (a^2)^2 \otimes a \text{ amallarini}$$

bajarish kerak.

Parametr R li darajaga oshirish amalini bajarish tezligini oshirish uchun parametrlar algebrasining $a^x \equiv ((1 + R * a)^x - 1) * R^{-1} \pmod{n}$ xossasidan foydalanish maqsadga muvofiq [3].

Keltirilgan amallar orqali bir tomonlama funksiyalarni hisoblash juda qulay, bu esa ushbu amallar orqali yangi kriptotalgoritmlarni yaratish yoki mavjud kriptotalgoritmlarni takomillashtirish imkonini beradi.

Butun sonli parametrli algebraik strukturalarga asoslangan bir tomonlama kriptografik funksiyalar kriptografiya sohasida qo'shimcha daraja parametriga asoslangan murakkablikni ham keltirib chiqaradi. Bu esa mavjud algoritmlarni yanada takomillashtirish va yangi kriptobardoshli algoritmlar ishlab chiqish imkonini beradi [3].

Parametrli algebaga asoslangan El-Gamal kriptografik tizimlari quyidagi jarayonlarni o'z ichiga oladi jarayonni o'z ichiga oladi:

Parametrli El-Gamal algoritmi:

Kalitlarni hosil qilish quyidagi qadamlardan iborat

1. Katta uzunlikdagi q tub sonini hosil qilinadi
2. $1 < x < q - 1$ shartni qanoatlantiruvchi maxfiy kalit, tasodifiy butun x sonni hosil qiladi.
3. $q < R$ shartni qanoatlantiruvchi va kalit x bilan o'zaro tub bo'lgan R parametr tanlab

olinadi. R parameter faqatgina xabar almashuvchilar o'rtasidagina ma'lum bo'lgan maxfiy kattalik.

4. Modul q dan kichik bo'lgan tasodifiy primitive a butun son tanlab olinadi.

5. $y = a^x \pmod{q}$ hisoblash amalga oshiriladi ya'ni R parameter bilan q modul bo'yicha a sonini x -darajaga oshiriladi. Parametr R bilan diadarajaga oshirish amali, $a^{x+1} \equiv a * \sum_{i=0}^{i=x} F^i \pmod{n}$ bunda $F = 1 + R * a$ [4]

6. Shundan so'ng $\{q, a, y\}$ ochiq kalit sifatida, x, R maxfiy kalit va parametr sifatida olinadi,

Shifrlash quyidagi qadamlardan iborat.

1. M ochiq ma'lumot q dan kichik bo'lgan bloklarga ajratiladi
2. $1 < k < q - 1$ shartni qanoatlantiruvchi va q bilan o'zaro tub bo'lgan k soni tasodifiy tanlab olinadi.
3. Diadarajaga oshirish amali oraqali $C_1 = a^k \pmod{q}$ va $C_2 = M * y^k \pmod{q}$ shifratmlar hisoblanadi.

Deshifrlash quyidagi qadamlardan iborat

4. Diadarajaga oshirish amali orqali $K = C_1^x \pmod{q}$ qiymat hisoblanadi.

Modul q bo'yicha K soniga teskari son K^{-1} hisoblanadi

$M = C_2 * K^{-1} \pmod{q}$ hisoblanib, M ochiq matn olinadi.

Natijalar. Parametrli algebraga asoslangan ochiq kalitli kriptografik algoritmnining gomomorfik xususiyatlarini ko'rib chiqamiz.

Parametrli El-Gamal algoritmining gomomorfik xususiyati:

Parametrli El-Gamal algoritmidan siklik guruh G uning tartibi q , asos g va maxfiy parametr R bo'lganda, ochiq kalit (G, q, g, y) ga teng. Bu yerda, $y = g^x \pmod{q}$, R, x esa maxfiy kalit. Bu holda ma'lumotni shifrlash funksiyasi $r \in \{0, \dots, q-1\}$ lar uchun $\varepsilon(m) = (g^r, m \cdot h^r)$ ga teng. Ushbu algoritm uchun gomomorfik xususiyat quyidagi teng bo'ladi.

$$\begin{aligned} \varepsilon(m_1) \cdot \varepsilon(m_2) &= (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) \\ &= ((g^{r_1+r_2}), (m_1 \cdot m_2)h^{r_1+r_2}) \\ &= \varepsilon(x_1 x_2) \end{aligned}$$



Bu yerda x^r amali R parametr bilan darajaga oshirish amali hisoblanadi.

Parametrlil algebra yordamida takomillashtirilgan El-Gamal kriptografik algoritmi shifrlash akslantirishlari va gomomorfik xususiyatlarini amalda tekshirish uchun algoritmlarning xususiy holdagi dasturlari yaratildi.

Dastur 4 qismdan iborat: Kalitlarni hosil qilish, xabarni shifrlash gomomorfik amal bajarish va xabarni deshifrlash.

Kalitlarni hosil qilish tasodifiy sonlar generatorlari orqali berilgan shartlar asosida amalga oshiriladi

1-rasm. Dasturning kalitlarni hosil qilish oynasi

El-Gamal algoritmidan farqli ravishda parametrli algebra asosidagi El-Gamal algoritmidagi maxfiy kalitlar x , parametr R oshkor qilinmaydi. x kalit shaxsiy kalit sifatida olinadi, R parametr esa faqat xabar almashinuvchilar o'rtasida ma'lum bo'ladi.

Xabarni shifrlash jarayoni ham parametrli algebra asosida amalga oshirildi.

2-rasm. Dasturning shifrlash oynasi

Shifrlangan matnlar ustida gomomorfik amal bajarish

3-rasm. Dasturning kalitlarni gomomorfik amal bajarish oynasi

Deshifrlash jarayonida ham ochiq matn va deshifrlangan matnlarni o'zaro mos kelishini aks etmoqda. Ushbu oynada deshifrlangan natija bilan ochiq matnlarning o'zaro ko'paytmasi bir xil ekanligini ko'rishimiz mumkin.

4-rasm. Dasturning deshifrlash oynasi

Muhokama. Dasturdagi funksional o'zgartirishlar va algoritmlarning bajarilish ketma-ketligini to'g'ri bajarilayotganligini anglatadi.

Parametrli algebra asoslangan El-Gamal shifrlash algoritmi diskret logarifmlash va faktorlash muammosiga qo'shimcha daraja parametri muammosini keltirib chiqaradi. Kriptografik algoritmi analiz qilish uchun maxfiy kalitlarni topish uchun yuqoridagilarga qo'shimcha daraja parametri R ni topish ham talab etiladi. Bu esa juda katta bo'lmagan uzunlikdagi kalitlar bilan yetarlicha bardoshlilikni ta'minlash imkonini beradi.

Butun sonli parametrli algebraik strukturalarga asoslangan bir tomonlama kriptografik funksiyalar kriptografiya sohasida yuqoridagi murakkabliklarga



qo'shimcha daraja parametriga asoslangan murakkablikni ham keltirib chiqaradi. Bu esa mavjud algoritmlarni yanada takomillashtirish va yangi kriptobardoshli algoritmlar ishlab chiqish imkonini beradi.

Xulosa. Xulosa qilib aytadigan bo'lsak, hozirda mavjud gomomorfik shifrlash algortimlarining kriptobardoshlilikiga juda katta sonlardan tashkil topgan kalitlarni generatsiya qilishga bog'liq. Albatta bu kalitlarning hajmi oshgan sari kriptobardoshlilik oshgani bilan bir vaqtda, ma'lumotni shifrlash va deshifrlash uchun ketadigan resurs va vaqt ham oshib boradi. Agar kalitlar uzunligi yetarli darajada uzun bo'lmasa maxsus algoritmi va hisoblash mashinalari yordamida maxfiy ma'lumotni oshkor qilish imkoniyati paydo bo'ladi. Shuning uchun paramertli algebra asosida mavjud algoritmlarning gomomorfik xususiyatlarini tadqiq etish nisbatan katta bo'lmagan uzunlikdagi kalit bilan yuqori bardoshlikka ega gomomorfik shifrlash algoritmlarini ishlab chiqish imkoniyatini beradi. Mazkur maqolada Parametrli algebra asoslangan El-Gamal shifrlash algoritmining gomorfik xususiyatlari tadqiq qilinib, yoritib berildi. Ushbu olingan natijalar bizga mavjud to'liq gomomorfik shifrlash algoritmlarini paramaetrli algebra amallari bilan takomillashtirib, bardoshlilikini yanada oshirish imkonini beradi.

Foydalanilgan adabiyotlar

1. Акбаров Давлатали Егиталиевич, Хасанов Пўлат Фаттохович, Хасанов Хислат Пўлатович, Ахмедова Ойдин Пўлатовна. (т.ф.д., профессор П.Ф. Хасанов тахрири остида) "Криптографиянинг математик асослари" – ТОШКЕНТ 2010. 210 б
2. William Stallings. Cryptography and Network Security: Principles and Practice, Sixth edition. Prentice Hall, 2014.
3. Xasanov X.P. Takomillashgan diamatristalar algebra va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari.– Toshkent, 2008. -208 b.
4. Хасанов Хислат Пулатович. Мавжуд криптоалгоритмларни параметрлар алгебраси асосида такомиллаштиришнинг умумий усули.

5. http://ru.infocom.uz/wp-content/download/information_security_24112005_17.html
6. Papisetty, S.D. (2017). Homomorphic Encryption: Working and Analytical Assessment : DGHV, HElib, Paillier, FHEW and HE in cloud security.
7. Xudoynazarov, U., & Meliquziyev, A. (2023). OCHIY KALITLI RSA SHIFRLASH ALGORITMINI PARAMETRLI ALGEBRA ASOSIDA TAKOMILLASHTIRISH. Research and implementation.

