MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

# "AL-FARG'ONIY 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

ISSN 2181-4252

# 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‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») 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



**FARG’ONA - 2023 YIL**

**Jurnal quyidagi bazalarda indekslanadi:**

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · DRJI Directory of Research Journals Indexing

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

# 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” kafedrasi 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 ololmaydi. 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 algebraga asosida takomillashtirilgan El-Gamal ochiq kalitli kriptografik algoritmining gomomorfik hususiyatlarini 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 безопастност 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 $m_1, m_2, \ldots . m_n$ kiruvchilar uchun $f(m_1, m_2, \ldots . m_n)$ natijani olmoqchi bo‘lsa,

uning o‘rniga $c_1, c_2, \dots c_n$ kiruvchi shifrmatn qiymatlarini hisoblash, $f(m_1, m_2, \dots \dots m_n)$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 shifr matnida bajarilishi mumkin bo‘lgan matematik operatsiyalarning turlari va chastotalariga bog‘liq. Gomomorfik shifrlashning uch turi bor:

- Qisman (Partially) gomomorfik shifrlash
- Qisman (Somewhat) homomorfik 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 shifr 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 yordmida faqat ko‘paytirish bilan bog‘liq gomomorfik amallarni bajarishimiz mumkin.

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

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

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

El-Gamal algoritmining kriptobardoshliligi 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 deshifrash jarayonlarini sekinlashtiradi.

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

**Parametrli algebra**. Ko‘p hollarda mavjud kriptografik algoritmlar parametrlar algebrasi asosida yaratilgan algoritmlarning hususiy holi bo‘lib qolmoqda.

**Parametrlar algebrasida asosiy amallar quyidagicha aniqlanadi:**

1) Parametr $R$ li ko‘paytirish amali

$a ® b \equiv a + b + a * R * b\ (mod\ \ n)R$

parametrlar algebrasida koeffitsiyent yoki parametr deb atalishi mumkin. $R = 0$ bo‘lganda bu ifoda klassik algebradagi qo‘shish amalini ifodalaydi.

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

Parametrlar algebrasida 0 birlik elementi hisoblanib, $a \circledR 0 \equiv a (mod\ n)$ xossaga ega.

3) Parametr $R$ li darajaga oshirish amali $a^{\backslash x+1} \equiv a * \sum_{i=0}^{i=x} F^{\,i} (mod\ n)$, bunda $F = 1 + R * a$.

$a^{\backslash 37}$ darajasini hisoblash uchun:

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

$$\left(\left(\left(\left(\left(a^{\backslash 2}\right)^{\backslash 2}\right)^{\overline{2}}\right)\right)^{\backslash 2}\right)^{\overline{2}} \circledR \left(a^{\backslash 2}\right)^{\backslash 2}) \circledR a$$

amallarini bajarish kerak.

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

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

Butun sonli parametrli algebraik strukturalarga asoslangan bir tomonlama kriptografik funksiyalar kriptografiya sohasida qo‘shimcha daraja parametriga asoslangan murakkablikni ham keltirb 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. $y = a^{\backslash x} mod q$ hisoblash amalga oshiriladi ya’ni $R$ parameter bilan $q$ modul bo‘yicha $a$ sonini $x$ -darajaga oshiriladi. Parametr $R$ bilan diadarajaga oshirish amali, $a^{\backslash x=1} \equiv a * \sum_{i=0}^{i=x} F(i) \ (mod\ n)$ 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 $C_1 = a^{\backslash k} \ modq$ va $C_2 = M * y^{\backslash k} mod\ q$ shifrmatnlar hisoblanadi.

**Deshifrlash quyidagi qadamlardan iborat**

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

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

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

***Natijalar.*** Parametrli algebraga asoslangan ochiq kalitli kriptografik algoritmning gomomorfik xususiyatlarini ko‘rib chiqamiz.

***Parametrli El-Gamal algoritmining gomomorfik xususiyati:***

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

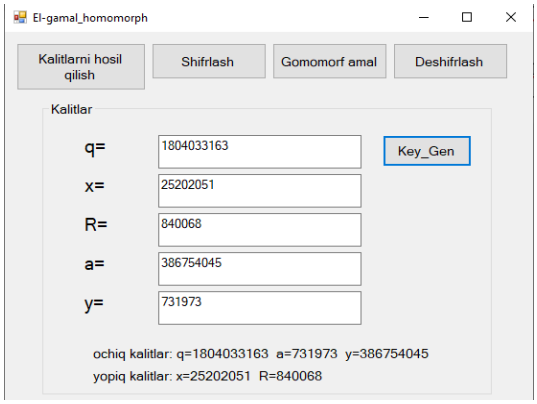
$$\begin{aligned} \varepsilon(m_1) \cdot \varepsilon(m_2) &= (g^{\backslash r_1}, m_1 \cdot h^{\backslash r_1})(g^{\backslash r_2}, m_2 \cdot h^{\backslash r_2}) \\ &= ((g^{\backslash (r_1 + r_2)}, (m_1 \cdot m_2) h^{(r_1 + r_2)}) \\ &= \varepsilon(x_1 x_2) \end{aligned}$$

Bu yerda $x^{\backslash r}$ amali $R$ parametr bilan darajaga oshirish amali hisoblanadi.

Parametrli algebraga 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.

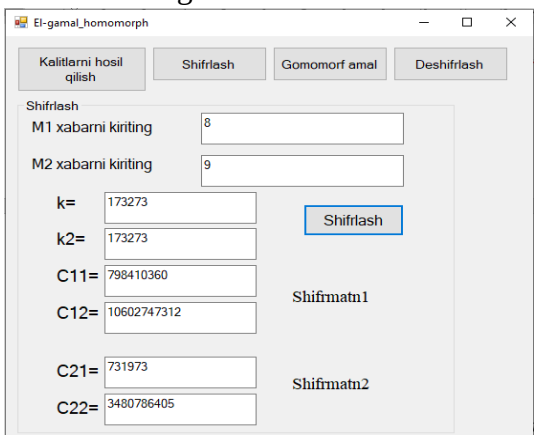
Kalitlarni hosil qilish tasodifiy sonlar generatorlari orqali berilgan shartlar asosida amalga oshiriladi




***1-rasm. Dasturning kalitlarni hosil qilish oynasi***

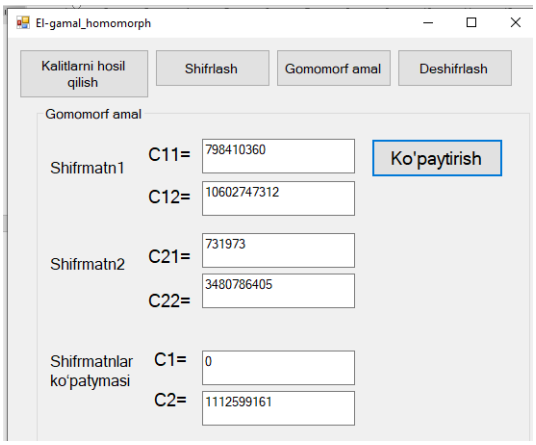
El-Gamal algoritmidan farqli ravishda parametrli algebra asosidagi El-Gamal algoritmida maxfiy kalitlar $x$, parametr $R$ oshkor qilinmaydi. $x$ kalit shaxsiy kalit sifatida olinadi, $R$ parametr esa faqat xabar almashinuvchilar o‘rtasida ma’lum bo‘ladi.

Xabarni shifrlash jarayoni ham parametrli algebra asosida amalga oshirildi.



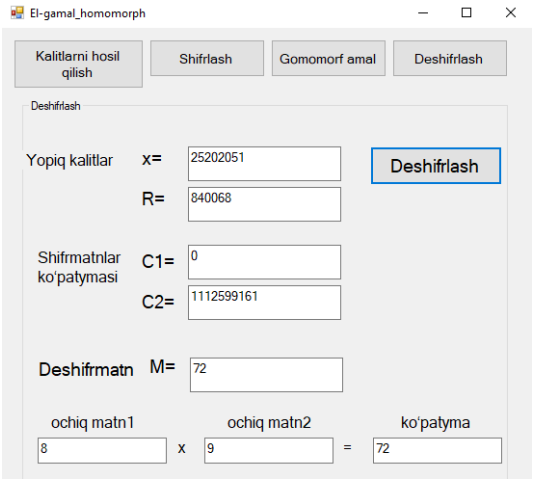

***2-rasm. Dasturning shifrlash oynasi***

Shifrlangan matnlar ustida gomomorf amal bajarish




***3-rasm. Dasturning kalitlarni gomomorf 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 algebraga asoslangan El-Gamal shifrlash algoritmi diskret logarifmlash va faktorlash muammosiga qo‘shimcha daraja parametri muammosini keltirib chiqaradi. Kriptografik algoritmni analiz qilish uchun maxfiy kalitlarni topish uchun yuqoridagilarga qo‘shimcha daraja pametri $R$ 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 keltirb 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 kriptobardoshliligi juda katta sonlardan tashkil topgan kalitlarni generatsiya qilishga bog’liq. Albatta bu kalitlarnig 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 algoritm 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 algebraga 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, bardoshliligini 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 таҳрири 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 algebralari 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). OCHIQ KALITLI RSA SHIFRLASH ALGORITMINI PARAMETRLI ALGEBRA ASOSIDA TAKOMILLASHTIRISH. Research and implementation.