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(8)
2024-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.

2024 yil, Tom 1, №4
Vol.1, Iss.4, 2024 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 - 2024 YIL

Jurnal quyidagi bazalarda indekslanadi:

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

YETARLI GOMOMORFIK SHIFRLASH ALGORITMLARI YORDAMIDA AXBOROTNI KRIPTOGRAFIK HIMOYALASH

Xudoykulov Z.T.,
Muhammad al-Alxorazmiy nomidagi Toshkent axborot texnologiyalari universiteti,
Toshkent, O‘zbekiston
zarif.khudoykulov@tuit.uz

Xudoynazarov U.U.,
Muhammad al-Alxorazmiy nomidagi Toshkent axborot texnologiyalari universiteti,
Toshkent, O‘zbekiston
umidjonxudoynazarov@gmail.com

Annotatsiya. An’anaviy shifrlash algoritmlari ma’lumotlarni saqlashda va uzatilishida axborot xavfsizligini ta’minlaydi, lekin, axborotga ishlov berish jarayonlarida konfidensiallikni ta’minlamaydi. Bunday muammo bulutli tuzilmalardagi zaifliklarning barchasini yoki hech bo‘lmaganda bir qismini bartaraf etadigan xavfsizlik tizimini yaratish vazifasini keltirib chiqaradi. Ushbu maqolada gomomorfik shifrlash algoritmlari va uning turlari, yetarli (somewhat) gomomorfik shifrlash algoritmlarining afzalliklari va ularni amalga oshirishdagi muammolar tahlil qilinadi.

Kalit so‘zlar. Gomomorfik shifrlash, yetarli gomomorfik shifrlash, elliptik egri chiziqlar, diskret logarifm, to‘liq gomomorfik shifrlash

Kirish. Gomomorfik shifrlash algoritmlarini elektron hukumat, xavfsizlik tizimlari, sog‘liqni saqlash, bulutli hisoblash tizimlari, buyumlar interneti tizimlari, suniy intellekt va mashinali o‘qitish kabi bir qancha sohalarda qo‘llash maxfiy ma’lumotlarni qayta ishlash jarayonida konfidensiallikni ta’minlaydi.

Gomomorfik shifrlash sxemasi bulutli tizimlarda shifrlangan ma’lumotlar ustida, ularni deshifrlamasdan amallarni bajarish mexanizmini ta’minlaydi. Bundan tashqari to‘liq gomomorfik shifrlash algoritmlari shifrlangan ma’lumotlar ustida ixtiyoriy amallarni bajarish imkonini beradi, shuning uchun gomomorfik shifrlash algoritmlari kriptografiyaning noyob elementi hisoblanadi[2].

Yaqin vaqtgacha shifrlangan ma’lumotlarni qayta ishlash muammosini qanoatlantiradigan umumiy foydalanish usuli mavjud emas edi. Rivest, Adleman va Dertouzos 1978-yilda shifrlangan ma’lumotlarda oddiy hisob-kitoblarni amalga oshirish mumkinmi degan savolni berib, *maxfiylik gomomorfizmi* tushunchasini kiritdilar. Keyinchalik Craig Gentri 2009-yilda chop etilgan doktorlik dissertatsiyasida birinchi to‘liq gomomorf shifrlash sxemasini taklif qilgan [2].

Adabiyotlar tahlili va metodologiya.

Maqolada hozirgi kunda axborot xavfsizligini ta’minlash usullari va vositalari yoritilgan adabiyotlar o‘rganib chiqildi. Ushbu sohada bir qancha olimlarning izlanish olib bormoqda. Jumladan R.Rivest, A.Shamir, L.Adleman[1], H.Goldvasser, Silvio Mikali[3], Taher Elgamal[4], Benaloh.J.C.[5], Pascal Paillier[6], Dan Boneh, Eu Jin Goh, Kobbi Nissim[7], Ayantika Chatterjee va Khin Mi Mi Aung[8], Stefan Rass va Daniel Slamanig[2], Chetin Kaya Koch, Funda O‘zdemir, Zeynep O‘demiş O‘zger[9], Jain, N., Cherukuri, A. K.[10], A.Wainakh, [11] va boshqa olimlar izlanishlar olib bormoqdalar.

Gomomorfik shifrlash sxemalari. Gomomorfik shifrlash algoritmlarining kelib chiqishi algebraik strukturalardagi “*Gomomorfizm*” tushunchasi bilan bog‘liq. “Gomomorfizm” atamasi yunoncha “*homos*” va “*morphe*” so‘zlaridan olingan bo‘lib, “bir xil” , “shakl” yoki “tuzilma” degan ma’noni anglatadi [10].

Shifrlangan matnlar ustida bajarilgan algebraik amallar (qo‘shish va ko‘paytirish) gomomorf shifrlash sxemalari orqali bajariladi va ichki ochiq matnga ta’sir qiladi. Bu shuni anglatadiki, ba’zi $(G_2,*)$ guruhning elementlari bo‘lgan $Encrypt(m_1;\ pk)$ va $Encrypt(m_2;\ pk)$ ikkita shifrlangan matnlari berilgan bo‘lsa, uchinchi tomon maxfiy kalitsiz va m_1, m_2 ochiq matnlarni bilmasdan shifrlangan matnlar ustida $Encrypt(m_1 \circ m_2;\ pk) = Encrypt(m_1;\ pk) * Encrypt(m_2;\ pk)$ algebraik amallarni hisoblashi mumkin [8].

Gomomorfik shifrlash algoritmlari turlari

Gomomorf shifrlash algoritmlarini *uch turga* bo‘lish mumkin [11]:

1. *Qisman (Partially)* gomomorfik shifrlash
2. Yetarli *(Somewhat)* gomomorfik shifrlash
3. *To‘liq (Fully)* gomomorfik shifrlash.

Ularning orasidagi asosiy farq shifr matnida bajarilishi mumkin bo‘lgan algebraik amallarning turlari va chastotalariga bog‘liq.

Materiallar va usullar. 2005-yilgacha barcha taklif qilingan gomomorf shifrlash sxemalari faqat qo‘shish yoki ko‘paytirish operatsiyalari bilan cheklangan. Yangi gomomorfik shifrlash sxemsiga yaqinlashadigan dastlabki harakatlar Boneh-Goh-Nissim (BGN) tomonidan taqdim etilgan [11]. BGN sxemasi bitta ko‘paytirish amali va cheksiz miqdordagi qo‘shish amallarini va doimiy o‘lchamdagi shifrlangan matnni qo‘llab-quvvatlaydi. Shu sababli, kriptografik tizim “yetarli gomomorf” deb ataladi [2].

BGN shifrlash sxemasining matematik asoslari.

Ushbu algoritmda to‘plamlar nazariyasi, guruh halqa, maydon, diskret logarifmlash, faktorlash va elliptik egri chiziqlar kabi matematik tushunchalardan foydalaniladi.

Ta’rif: Additiv chekli Abel guruhlariga tegishli G_1, G_2 va multiplikativ chekli Abel guruhiga tegishli G_3 guruhlar olingan bo‘lsin. Ikki chiziqli juftlashtirish bu quyidagi holatlar uchun $e: G_1 \times G_2 \to G_3$ akslantirishdir:

(*Ikki chiziqlilik*) Ixtiyoriy $P, Q \in G_1$ va $R \in G_2$ ratsional nuqtalar uchun quyidagi ifodalar o‘rinli

$$e(P+Q, R) = e(P, R) \times e(Q, R).$$

Shunga o‘xshash Ixtiyoriy $P \in G_1$ va $Q, R \in G_2$ ratsional nuqtalar uchun quyidagi ifodalar o‘rinli

$$e(P, Q+R) = e(P, Q) \times e(P, R)$$

Berilgan maydondagi elliptik egri chiziqlar nuqtalari ustida ushbu amallar ikki chiziqli juftlikni ifodalaydi [9].

***n* -tartibli ikki chiziqli guruhni qurish.** Boneh, Goh va Nissim ikki chiziqli xaritani qo‘llab-quvvatlovchi guruh bo‘lgan berilgan n −tartibli ikki chiziqli G guruhini qurishning quyidagi usulini ta’riflagan [7].

3 ga bo‘linmaydigan $n > 3$ shartni qanoatlantiruvchi butun kvadratik son berilgan bo‘lsin.

I) Eng kichik butun musbat $l \in Z$ soni tanlab olinadi hamda $p = l \times n - 1$ va $p \equiv 2(mod\ 3)$ shartni qanoatlantiruvchi p tub son hosil qilinadi.

II) Z_p maydonga tegishli $y^2 = x^3 + x$ elliptik egri chiziqning ratsional nuqtalari ko‘rib chiqiladi. $p \equiv 2\ mod\ 3$ ifodadan, elliptik egri chiziq $Z_p \times Z_p$ maydonda $p + 1 = l \times n$ nuqtaga ega bo‘ladi. Shuning uchun egri chiziqdagi nuqtalar guruhi $n-$ tartibli kichik guruhga ega bo‘lib, u G bilan belgilanadi.

III) $Z^*_{p^2}$ to‘plamning qismguruhi bo‘lgan $n-$ tartibli G' to‘plamn olaylik. Elliptik egri chiziqlardagi o‘zgartirilgan Weil juftligi kerakli xususiyatlarga ega $e: G \times G \to G'$ ikki chiziqli akslantirishni beradi.

BGN tizimidagi asosiy g‘oyalardan biri elliptik egri chiziq guruhlardan foydalanishdir. Guruh tartibi n murakkab son bo‘lib, uni faktorlash qiyin. Oldingi barcha tizimlarda guruh tartibi tub bo‘lishi talab qilingan.

Barcha gomomorfik shifrlash algoritmlari kabi BGN tizimi ham *kalitlarni hosil qilish*, *xabarni shifrlash*, *gomomorfik amal bajarish* va *xabarni deshifrlash* jarayonlaridan iborat.

Kalitlarni hosil qilish.

Dastlab qulaylik uchun elliptik egri chiziqlarning qo‘shish amalini “×” bilan belgilab olinadi hamda $[a]P$ ko‘paytirish amali P^a bilan belgilab olinadi.

Kalitlarni yaratish quyidagi bosqichlarni o‘z ichiga oladi.

1. Xavfsizlik parametrlarini kiritishda q_1 va q_2 ehtimollik boshlang‘ich qiymatlar tanlanadi va $n = q_1 \cdot q_2$ hisoblanadi.
2. Eng kichik butun musbal l soni tanlab olinadi va $p = l \times n - 1$ butun tub son hisoblanadi.
3. $n = q_1 \times q_2$ tartibli $\mathcal{E}(Z_p)$ to‘plamning qismguruhi bo‘lgan G siklik guruh va $Z^*_{p^2}$ guruhning qismguruhi bo‘lgan G' uchun $e: G \times G \to G'$ ikki chiziqli juftlashtirish hosil qilinadi.
4. G guruhga tegishli bo‘lgan ikkita turli tasodifiy g, u generatorlar tanlanadi va $h = u^{q_2}$ qiymat hosil qilinadi. Bu yerda, h qiymat tartibi q_1 bo‘lgan G guruhning qismguruhidir.
5. Ochiq kalit sifatida $p_k = (n, G, G_T, e, g, h)$ olinadi va maxfiy kalit sifatida $s_k = q_1$ olinadi.

Xabarni shifrlash. M ochiq matn belgilari $m \in Z_{q^2}$ raqamli ko‘rinishga o‘tkaziladi hamda tasodifiy $r \in_R Z_n$ soni tanlanadi. Keyin c shifrmatn quyidagicha hisoblanadi:

$$c = g^m h^r mod\ n \in G$$

Har bir jo‘natilgan m xabar uchun r qiymat tasodifiy tanlanadi.

Xabarni deshifrlash. Yopiq kalit $s_k = q_1$ va shifrmatn c berilgan bo‘lsin.

Ochiq matn m quyidagicha tiklanadi:

$$c^{q_1} = (g^m \times h^r)^{q_1} = (g^m)^{q_1} \times (h^r)^{q_1}$$
$$= (g^m)^{q_1} \times ((u^{q_2})^r)^{q_1}$$
$$= (g^{q_1})^m \times (u^{q_1 \times q_2})^r = (g^{q_1})^m \in G$$

Xabarlar fazosi polinomial chegaralanganligi uchun ochiq matn m quyidagicha hisoblanadi:

$$m = \log_{g^{q_1}} c^{q_1}$$

Samarali shifrni ochish uchun diskret logarifm shifrni ochish jarayoniga tezlik chegarasini qo‘yishi sababli xabar maydoni kichik bo‘lishi kerak.

Boneh-Goh-Nissim (BGN) shifrlash algoritmining gomomorfik xususiyati. Yetarli gomomorfik shifrlash algoritm sifatida, ushbu shifrlash sxemasi shifrmatnlar ustida ixtiyoriy qo‘shish amallarini va faqat bir martagina ko‘paytirish amalini bajarish imkonini beradi [2].

Ko‘paytirishdan oldingi qo‘shish amali. m_1, m_2 xabarlari uchun c_1, c_2 shifrlangan matnlar va mos ravishda r_1, r_2 randomizatorlar berilgan bo‘lsa, yangi randomizator $r \in Z_n$ tanlanadi va quyidagi hisoblanadi

$$E_g(m_1, r_1) \times E_g(m_2 \times r_2) = (g^{m_1} \times h^{r_1}) \times (g^{m_2} \times h^{r_2}) = g^{m_1+m_2} \times h^{r_1+r_2}) = E_g(m_1 + m_2, r_1 + r_2),$$

Bu yerda, $m_1 + m_2$ xabarlarning tasodifiyligi $r_1 + r_2$ ga teng.

Agar shifrlash funksiyasini $E_g(m, r) = E(m)$ tarzida belgilansa, u holda m_1 va m_2 xabarlar uchun quyidagiga ega erishiladi.

$$D\big(E(m_1 + m_2)\big) = D(E(m_1) \times E(m_2)),$$

Bu yerda, D eshifrlash funksiyasini anglatadi.

Ko‘paytirish. r tasodifiy qiymatli m xabar va skalyar k soni uchun, skalyar ko‘paytirish $k \times m$ tasodifiylikni $k \times r$ ga almashtirish orqali amalga oshiriladi.

$$(E_g(m, r))^k = (g^m \times h^r)^k = g^{k \times m} \times h^{k \times r}$$
$$= E_g(k \times m, k \times r)$$

Bu ifodani quyidagicha ifodalash mumkin

$$D\big(E(k \times m)\big) = D\left(\big(E(m)\big)^k\right).$$

BGN algoritmi shifrlash funksiyasining asosini va sohasini bir marta o‘zgartirish orqali ochiq matnlarni bir marta ko‘paytirish imkonini beradi. g va u qiymatlar G guruhning elementi va $h = u^{q_2}$ bo‘lganligidan biron bir $\alpha < n$ son uchun $g^\alpha = h$ qiymat olinadi. Faraz qilaylik $e: G \times G \to G'$ ikki chiziqlik juftlik bo‘lsin va $e(g, g) = g'$, $e(g, h) = h'$ ifoda o‘rinli bo‘lsin. U holda

$$h' = e(g, h) = e(g, g^\alpha) = e(g, g)^\alpha = (g')^\alpha.$$

g qiymat G guruhning elementi $e(g,g)=g'$ qiymat esa tartibi n bo‘lgan G' guruhning elementi ekanini e’tiborga olinsa, u holda

$$E_{g'}: Z_{q_2} \times Z_n \to G'$$
$$(m,r) \to (g')^m \times (h')^r$$

Ikkita $c_1 = E_g(m_1, r_1)$ va $c_2 = (m_2, r_2)$ shifrlangan xabarni g asosi bilan $m_1 \times m_2$ ko‘paytmaning haqiqiy shifrlanishini g asosi bilan birlashtiriladi.

$e(c_1,c_2)\times(h')^r = e(g^{m_1}\times h^{r_1}, g^{m_2}\times h^{r_2})\times(h')^r =$
$e(g^{m_1}\times(g^{\alpha})^{r_1}, g^{m_2}\times(g^{\alpha})^{r_2})\times(h')^r =$
$e(g^{m_1}\times g^{\alpha\times r_1}, g^{m_2}\times g^{\alpha\times r_2})\times(h')^r$
$= e(g^{m_1+\alpha\times r_1}, e(g^{m_2+\alpha\times r_2})\times(h')^r =$
$e(g,g)^{(m_1+\alpha\times r_1)\times(m_2+\alpha\times r_2)}\times(h')^r$
$= (g')^{(m_1+\alpha\times r_1)\times(m_2+\alpha\times r_2)}\times(h')^r =$
$(g')^{m_1\times m_2+\alpha\times m_1\times r_2\alpha\times m_2\times r_1+\alpha^2\times r_1\times r_2}\times(h')^r =$
$(g')^{m_1\times m_2+\alpha\times(m_1\times r_2+m_2\times r_1+\alpha\times r_1\times r_2)}\times(h')^r =$
$(g')^{m_1\times m_2}\times(g')^{\alpha\times(m_1\times r_2+m_2\times r_1+\alpha\times r_1\times r_2)}\times(h')^r =$
$(g')^{m_1\times m_2}\times((g')^{\alpha})^{m_1\times r_2+m_2\times r_1+\alpha\times r_1\times r_2}\times(h')^r =$
$(g')^{m_1\times m_2}\times(h')^{m_1\times r_2+m_2\times r_1+\alpha\times r_1\times r_2}\times$
$(h')^r =$
$(g')^{m_1\times m_2}\times(h')^{m_1\times r_2+m_2\times r_1+\alpha\times r_1\times r_2+r}$
$= (g')^{m_1\times m_2}\times(h')^{\bar{r}} =$
$E_{g'}(m_1\times m_2, \bar{r})$.

Berilgan $E_{g'}(m_1\times m_2,\bar{r})$ ifoda $m_1\times m_2$ ochiq matnlarning ayni ko‘paytmasining shifrlanganini hisoblanadi. Bu ko‘paytirish faqat bir marta amalga oshirilishi mumkin, chunki $G'\times G'$dan boshqa n tartibli guruhga e' ning ikki chiziqli juftligi mavjud emas.

Boshqa tomondan $D\big(E(m_1\times m_2)\big) = D\big(E(m_1)\times E(m_2)\big)$ munosabat o‘rinli bo‘ladigan ko‘paytirish amali ikkinchi marta mavjud bo‘lmaydi. Shuning uchun BGN multiplikativ jihatdan gomomorfik deb hisoblanmaydi. Chunki gomomorfik ko‘paytirish amali bir marta bajariladi holos.

Ko‘paytirishdan keyingi qo‘shish amali. Ikki chiziqli juftlik e yordamida va BGNning additiv gomomorfik xossalaridan foydalanib, ochiq matnli xabarlarni bir marta ko‘paytirishdan oldin va keyin istalgancha qo‘shishni amalga oshirish mumkin.

BGN algoritmining yana bir gomomorfik xususiyati bu o‘zgarmas son bilan qo‘shish amalidir:

$E_g(m+k,r) = g^{m+k}\times(h)^r = (g^m\times g^k)\times h^r = (g^m\times h^r)\times g^k = c\times g^k$. Bu esa quyidagini ko‘rsatadi

$$D\big(E(k+m)\big) = D(E(m)\times g^k)$$

BGN algoritmini tekshirish uchun quyidagi misol ko‘rib chiqiladi.

Kalitlarni hosil qilish. Kalitlarni hosil qilish uchun dastlab siklik guruh qurib olinadi. Buning uchun $q_1 = 7$ va $q_2 = 11$ butun sonlar tanlab olinadi va $n = q_1\cdot q_2 = 7*11 = 77$ hisoblanadi. Keyin ikki chiziqli akslantirishga ega elliptik egri chiziq guruhi quriladi. Butun sonlar to‘plamiga tegishli $l=4$ soni tanlanadi va $p = 3\,mod 4$ shartni qanoatlantiruvchi $p = 4*77-1 = 307$ maydon aniqlab olinadi. Natijada n=308/4=77 tartibli G kichik guruhni o‘z ichiga olgan, $E(p) = p+1 = 308$ ratsional nuqtalar bilan hosil qilingan elliptik egri chiziq supersingulyar hisoblanadi. G guruhga tegishli ikkita tasodifiy $g = [182{,}240]$, $u = [182{,}240]^{48} = [28{,}262]$ nuqtalar tanlab olinadi. Elliptik egri chiziq ratsional nuqtalarini b soniga ko‘paytirish amali $[a,b]^b$ kabi belgilab olinadi. Bu yerda, g va u generatorlar $y^2 = x^3 + x\ mod\ 307$ elliptik egri chiziqning $n=77$ tartibga ega nuqtalari. Keyin G qismguruhning q_1 tartibli $h = u^{q_2} = [28{,}262]^{11} = [99{,}120]$ tasodifiy son hosil qilinadi. Bu yerda, $p_k = (n, G, G_1, f, g, h)$ ochiq kalit sifatida, $s_k = q_1$ maxfiy kalit sifatida olonadi.

Xabarni shifrlash. Shifrlash uchun $m=3$ qiymat olinadi. Ixtiyoriy $r=2$ soni olinadi hamda shifrmatn hisoblanadi:

$C = g^M h^r = [182{,}240]^3 \times [99{,}120]^2\ mod\ 307 = [287{,}283]\times[175{,}229] = [177{,}88]$.

Bu yerda, “×” chekli maydonda elliptiktik egri chiziqning ratsional nuqtalarini qo‘shish amali.

Shifrmatnni deshifrlash. Shifrmatnni deshifrlash dastlab g^{q_1} ning diskret logarifmi hisoblab chiqiladi:

$g' = g^{q_1}$.
$g'^1 = [182{,}240]^7 = [146{,}60]$
$g'^2 = [146{,}60]^7 = [299{,}44]$

$$g'^3 = [272,206]$$
$$g'^4 = [191,151]$$
$$g'^5 = [79,171]$$
$$g'^6 = [79,136]$$
$$g'^7 = [191,156]$$
$$g'^8 = [272,101]$$
$$g'^9 = [299,263]$$
$$g'^{10} = [146,247]$$
$$g'^7 = \infty$$

Deshifrlash formulasi hisoblanadi: $C^{q_1} = (M^r h^r)^{q_1} = (g^{q_1})^M = [272,206]$ hisoblanadi. Hosil qilingan ifodadan m ochiq matn diskret logarifmlash orqali hisoblanadi. Hosil bo‘lgan qiymat $C^{q_1} = g'^3$ ga to‘g‘ri keladi. Demak, ochiq matn $m = 3$ ga teng.

BGN algoritmining gomomorfik xususiyati. Gomomorfik xususiyatlarni tekshirish uchun $m_1 = 3$, $m_2 = 2$, $r_1 = 2$, $r_2 = 3$ butun qiymatlar olinadi va C_1 va C_2 shifrmatnlar hisoblanadi:

$$C_1 = g^{m_1} \times h^{r_1} = [182,240]^3 \times [99,120]^2 = [177,88]$$
$$C_2 = C_1 = g^{m_2} \times h^{r_2} = [182,240]^2 \times [99,120]^3 = [259,143] \times [40,106] = [277,39]$$

Shifrmatnlar ustida qo‘shish amali bajariladi: $E_g(m_1, r_1) \times E_g(m_2, r_2) = [177,88] \times [277,39] = [294,218]$.

Ochiq matnlar yig‘indisini hisoblash $E_g(m_1 + m_2, r_1 + r_2) = E_g(5,5) = [182,240]^{2+3} \times [99,120]^{3+2} = [294,218]$. Bundan kelib chiqadiki $m_1 + m_2 = 2 + 3 = 5$ ga teng.

Muhokama Hozirda mavjud qisman gomomorfik shifrlash algoritmlari *chekli maydonda sonlarni diskret logarifmlash*, *katta sonlarni tub ko‘paytuvchilarga ajratish*, chekli maydonda elliptik egri chiziqlarning ratsional nuqtalarini aniqlash muammosiga asoslanadi.

Yetarli gomomorfik shifrlash algoritmlarining aksariyati ham yuqoridagi matematik muammolarga asoslanadi va ushbu turdagi algoritmlarda ham yetarlicha kalit uzunligida tezkor, yuqori kriptobardoshlikka ega gomomorfik shifrlash algoritmlarni shakllantirish masalasi mavjud.

Yetarli gomomorfik shifrlash algoritmlarini takomillashtirish va algebraik amallar bajarib, ushbu algoritmlarni to‘liq gomomorfik shifrlash algoritmlari ko‘rinishiga o‘tkazish mumkin.

Xulosa. BGN kriptotizimi chekli maydonda elliptik egri chiziqlarning ratsional nuqtalarini aniqlash, diskret logarifmlash va qismguruhni aniqlash muammosiga asoslangangan. Ushbu amallar esa bugungi kunda kriptografiyada kam uzunlikda kalit va hisoblash resursi bilan kriptografik amallar bajarish imkoniyatini beradi. Yetarli gomomorfik shifrlash algoritmlarida amallar soni cheklangan bo‘lsada, bu algoritmlarni arifmetik amallar soni cheklanmagan to‘liq gomomorfik shifrlash algoritmlariga o‘tkazish imkoni mavjud. Shuning uchun yetarli gomomorfik shifrlash usullarini takomillashtirish o‘z navbatida to‘liq gomomorfik shifrlash algotirmlarini ham bardoshliligini oshishiga zamin yaratadi.

Amaliyotda qisman gomomorfik shifrlash algoritmlariga oid LighPHE, libhcs, paillier, Microsoft SEAL kabi kriptografik kutubxonalari mavjud. BGN shifrlash sxemasi kichik hajmdagi tahlillar va hisoblashlar uchun foydali, masalan, elektron ovoz berish (e-voting) yoki shifrlangan ma’lumotlarni qidirish (encrypted search) kabi sohalarda qo‘llaniladi. Masalan ovoz berish tizimlarida, saylovchilarning tanlovlarini shifrlangan holda qo‘shib borish va umumiy natijani olish mumkin.

Foydalanilgan adabiyotlar

1. Rivest R. L. et al. On data banks and privacy homomorphisms //Foundations of secure computation. – 1978. – T. 4. – №. 11. – C. 169-180.
2. Rass S., Slamanig D. Cryptography for security and privacy in cloud computing. – Artech House, 2013.
3. Shafi G., Micali S. Probabilistic encryption //Journal of computer and system sciences. – 1984. – T. 28. – №. 2. – C. 270-299.
4. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms //IEEE transactions on information theory. – 1985. – T. 31. – №. 4. – C. 469-472.

5. Benaloh J. Dense probabilistic encryption //Proceedings of the workshop on selected areas of cryptography. – 1994. – С. 120-128.
6. Paillier P. Public-key cryptosystems based on composite degree residuosity classes //International conference on the theory and applications of cryptographic techniques. – Berlin, Heidelberg: Springer Berlin Heidelberg, 1999. – С. 223-238.
7. Boneh D., Goh E. J., Nissim K. Evaluating 2-DNF formulas on ciphertexts //Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2. – Springer Berlin Heidelberg, 2005. – С. 325-341.
8. Chatterjee A., Aung K. M. M. Fully homomorphic encryption in real world applications. – Singapore: Springer, 2019.
9. Koç Ç. K., Özdemir F., Özger Z. Ö. Partially Homomorphic Encryption. – Springer, 2021. – С. 37-41.
10. Jain N., Cherukuri A. K. Revisiting Fully Homomorphic Encryption Schemes //arXiv preprint arXiv:2305.05904. – 2023.
11. Wainakh A. Homomorphic encryption for data security in cloud computing: дис. – Middle East Technical University, 2018.