UO‘K 004.056.55

GOMOMORFIK SHIFRLASH ALGORITMLARINING UMUMIY TAHLILI

Xudoykulov Z.T.[1], *Xudoynazarov U.U.*[1]

[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
zarif.khudoykulov@tuit.uz, umidjonxudoynazarov@gmail.com

Annotatsiya. *Buyumlar Interneti, bulutli hisoblash tizimlari, elektron hukumat, sun’iy intellekt ilovalari va neyron tarmoqlari tomonidan amalga oshirilgan hisoblash tizimlarida ma’lumotlar maxfiyligi bilan bog‘liq muammolar sezilarli darajada oshib bormoqda. Gomomorfik shifrlash algoritmlari shifrlangan ma’lumotlar ustida ularni deshifrlamasdan algebraik amallar bajarish imkoniyatini beradi. Ushbu maqolada gomomorfik shifrlash algoritmlarini tushunish uchun zarur bo‘lgan algebraik asoslari o‘rganib chiqilgan. Maqolada turli matematik muammolarga asoslangan asosiy to‘liq gomomorfik shifrlash sxemalari hamda ularning fundamental asoslari tavsiflangan. Gomomorfik shifrlash algoritmlariga oid kriptografik kutubxonalar va ularni amalga oshirish bilan bog‘liq muammolar tahlil qilingan.*

Kalit so‘zlar: *Gomomorfik shifrlash, to‘liq gomomorfik shifrlash, El-Gamal algoritmi, panjaralar, ideal panjara, faktorlash, algebraik strukturalar, bulutli hisolash.*

I. KIRISH

An’anaviy shifrlash texnologiyalari 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.

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

Yaqin vaqtgacha shifrlangan ma’lumotlarni qayta ishlash muammosini hal qilish uchun qoniqarli 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 [18]. 30 yildan ko‘proq vaqt davomida 2009-yilgacha ushbu kontseptsiya kriptografiyaning muqaddas g‘oyasi deb hisoblangan. Craig Gentri 2009-yilda chop etilgan doktorlik dissertatsiyasida birinchi to‘liq gomomorf shifrlash sxemasini taklif qilgan [2].

Bulutli hisoblash tizimlarida gomomorf shifrlashdan foydalanish konfidensial ma’lumotlar ustida bajariladigan hisob-kitoblarni maxfiyligi uchun juda muhim hisoblanadi [3].

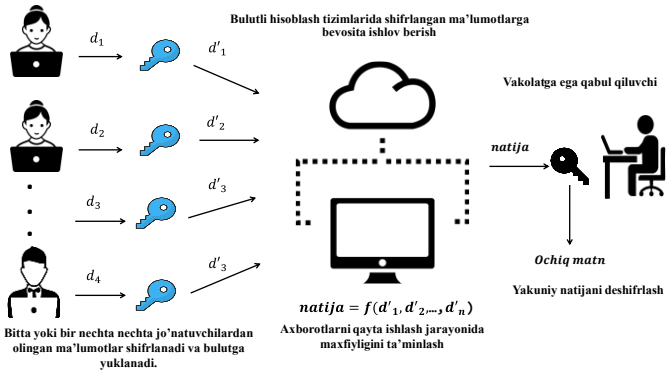
Bulutli hisoblash tizimlarida shifrlangan ma’lumotlar ustida ixtiyoriy amallar bajarilishi 1-rasmda ko‘rsatib o‘tilgan [3]. Faraz qilaylik mijoz maxfiy ma’lumotni bulutli hisoblash serverida qayta ishlamoqchi. Bunda hisoblash serveri ma’lumotni qayta ishlab yana mijozga jo‘natadi. Bu hisoblash *gomomorfik shifrlash algoritmi* yordamida yoki *gomomorfik shifrlash algoritmisiz* amalga oshirish mumkin [4].

Gomomorfik shifrlashsiz mijoz server texnologiyasi sxemasi 2-rasmda ko‘rsatilgan. Ushbu senariyda, server *M* ochiq xabarni ko‘rishi mumkinligi sababli, bu mijoz uchun katta xavfsizlik tahdidini keltirib chiqarishi mumkin. Maxfiy ma’lumotlar bilan ishlashda serverning maxfiy ma’lumotlarni ochiq xolda qayta ishlanishiga yo‘l qo‘ymaslik kerak.

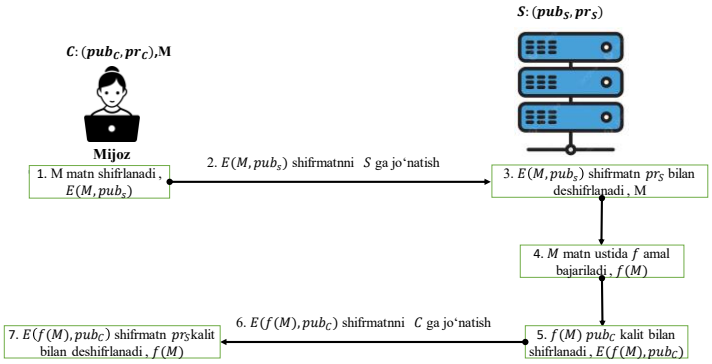
Gomomorfik shifrlash bilan mijoz server texnologiyasi sxemasi 3-rasmda ko‘rsatilgan.

Oddiy shifrlash algoritmlaridan farqli ravishda, bu yerda server o‘z ishini ko‘r-ko‘rona amalga oshiradi, chunki asl xabar shifrlangan holda bo‘ladi. Mijoz xabarining ma’nosi jamoatchilik uchun ham, server uchun ham noma’lumligicha qoladi [4].

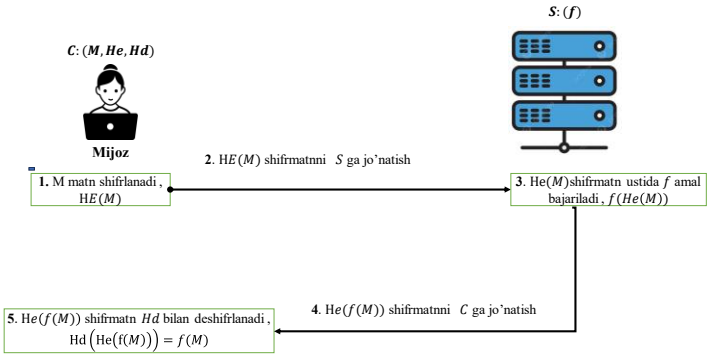
Quyida 1-3 rasmlarda maxfiy axborotlarni bulutli tizimlarda qayta ishlash jarayonlarida konfidensialligini saqlab qolish uchun gomomorfik shifrlash usullarini qo‘llash sxemasi keltirib o‘tiladi.



1-rasm. Bulutli hisoblash tizimida to‘liq gomomorfik shifrlash jarayoni



2-rasm. Gomomorfik shifrlashsiz mijoz server sxemasi



3-rasm. Gomomorfik shifrlashsiz mijoz server sxemasi

Mazkur maqolada gomomorfik shifrlash (GSH) algoritmlari va uning matematik asoslari, gomomorfik shifrlash algoritmlari turlari, gomomorfik shifrlash algoritmlarning amalda qo‘llanilishi sohalari, gomomorfik shifrlashga oid frameworklar va kutubxonalarni tavsiflash, gomomorfik shifrlash algoritmlariga oid muammolar va ularning kamchiliklari tahlil qilinadi.

II. ASOSIY QISM

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 [4].

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

$$Encrypt(m_1 \circ m_2, pk) = E$$

$$ncrypt(m_1, pk) * Encrypt(m_2, pk)$$

algebraik amallarni hisoblashi mumkin [5].

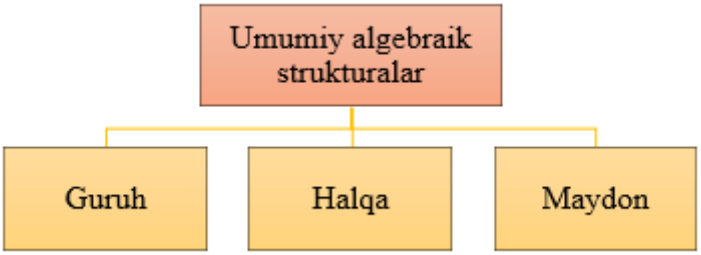
Bu shuni anglatadiki, shifrlangan matnlar ustida amallarni qayta-qayta bajarish mumkin, natijada har doim boshqa shifrlmatn hosil bo‘ladi. Agar yakuniy shifrmatn deshifrlansa, natijani aks ettiruvchi ochiq matnga ega bo‘linadi va bu dastlabki ochiq matnlar ustida barcha tegishli amallarni bajargandagi holat bilan bir xil bo‘ladi [3].

Gomomorfik shifrlash algoritmlarini matematik asoslari ifodalashda modul arifmetiksi, sonlar nazariyasi, ehtimollar nazariyasi, murakkablik nazariyasi, ideal panajaralar, matritsalar va elliptik egri chiziqlar nazaryasi elementlaridan tashkil topgan.

Agar biron to‘plam ma’lum to‘plamga gomomorf tarzda akslantirish mumkin bo‘lsa, bir to‘plamning ma’lum xususiyatlari ikkinchisiga qo‘llanilishi mumkin bo‘ladi, bu esa yangi to‘plamni tahlil qilishni soddalashtiradi. Gomomorfizm bu ikkita algebraik strukturalar o‘rtasidagi o‘zaro muvofiqlikni ifodalaydi [4].

Bir va undan ortiq amallar aniqlangan biror G-to‘plam *algebraik tizim yoki algebraik struktura* deyiladi.

Quyida uchta umumiy algebraik strukturalar: gruppa, halqa va maydon bilan tanishiladi.



4-rasm. Algebraik strukturalar

Guruh. Beshta xususiyatni (yoki aksiomani) qanoatlantiradigan va ko‘paytirish binar “•” amaliga ega bo‘lgan elementlar to‘plami *guruh* deyiladi va G bilan belgilanadi.

Abel guruhi deb ham ataladigan *kommutativ guruh* - bu operator guruhning berilgan xassalariga va kommutativlik xossasiga ega bo‘lgan guruhdir [8].

Ushbu besh xususiyat quyida tavsiflanadi:

- *Yopiqlik*;
- *Assotsiativlik*;
- *Kommutativlik*;
- *Neytral elementning mavjudligi*;
- *Teskari elementning mavjudligi*.

Agar G chekli bo‘lsa, G to‘plam chekli deb ataladi. Chekli guruhdagi elementlar soni uning *tartibi* deb ataladi.

Halqa. Halqa $(R,+,\times)$ bu- R to‘plam va qo‘shish $(+)$, ko‘paytirish $(\times)$ kabi binar amallardan iborat bo‘lib, quyidagi aksiomalar o‘rinli.

To‘plam elementlari ustiga bajariladigan *qo‘shish* amali uchun algebraik 3 ta xossa, *ko‘paytirish* amali uchun ham yuqoridagi 5 ta xossa o‘rinli bo‘lsa, bunday $(G,\bullet,+)$ algebraik tuzilma halqani tashkil etadi deyiladi.

Maydon. Biror G-to‘plamda ikkita “+” - qo‘shish va “·” - ko‘paytirish binar amallar (munosabatlar) aniqlangan bo‘lib, quyidagi quyidagi aksiomalar o‘rinli:

To‘plam elemenrlari ustiga bajariladigan *qo‘shish* amali uchun ham, *ko‘paytirish* amali uchun ham yuqoridagi 5 ta xossa o‘rinli bo‘lsa, bunday $(G,\bullet,+)$ algebraik tuzilma maydon tashkil etadi deyiladi.

Gomomorfik shifrlash turlari. Gomomorf shifrlash algoritmlarini *uch turga* bo‘lish mumkin.

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

Qisman (Partially) gomomorfik shifrlash

Chegaralangan (Somewhat) gomomorfik shifrlash *To‘liq (Fully)* gomomorfik shifrlash.

1-jadvalda Gomomorfik shifrlash algoritmlari turlariga mos amallar keltirilgan [9].

Qisman gomomorfik shifrlash (PHE) faqat bir turdagi algebraik amallar kerakli darajada ko‘p marta bajarishni qo‘llab-quvvatlaydi.

Qisman gomomorf shifrlash (PHE) sxemalari faqat qo‘shimcha operatsiyalarni qo‘llab-quvvatlasa *addidtive gomomorf sxema* yoki shifrlangan ma’lumotlarda faqat multiplikativ operatsiyalarni qo‘llab-quvvatlasa, *multiplikativ gomomorf sxema* deyiladi.

1-jadval. Gomomorfik shifrlashda amallar

Gomomorfik shifrlash turi	Bajariladigan amal	Amallar soni
Qisman gomomorfik shifrlash (PHE)	Bitta (qo‘shish yoki ko‘paytirish)	Cheklanmagan
Chegaralangan gomomorfik shifrlash (SWHE)	Ikkita (qo‘shish va ko‘paytirish)	Cheklangan
To‘liq gomomorfik shifrlash (FHE)	Ikkita (qo‘shish va ko‘paytirish)	Cheklanmagan

Qisman gomomorfik shifrlash sxemalariga RSA, El-Gamal, Paillier, Goldvasser-Mikali, Benaloh, Naccache-Stern, Damgard-Jurik, Okamoto Uchiyama, Sander-Young-Yung va boshqa bir qancha shifrlash algoritmlarini misol keltirish mumkin [2]. Ushbu algoritmlardan bir nechtasini shifrlash usullari va gomomorfik xususiyatlari quyida keltiriladi.

El-Gamal algoritmi. El-Gamal kriptografik tizimi uchta jarayonni o‘z ichiga oladi:

Kalitlarni hosil qilish. $q-$ tub son tanlanadi; $a<q$ shartni qanoatlantiruvchi a butun son tanlanadi; maxfiy kalit sifatida $1<x<q$ shartni qanoatlantiruvchi butun son tanlanadi; $y=a^x \bmod q$ hisoblanadi, ochiq kalitlar jufti q,a,y ma’lumotni shifrlovchi tomonlarga yoki ixtiyoriy odamlarga tarqatiladi.

Matnni shifrlash. q sonidan kichik bo‘lgan va $EKUB(k,q-1)=1$ shartni bajaruvchi $k-$ sonini tanlab olinadi; k son asosida $C_1=a^k \bmod q$ hisoblanadi; ochiq matnning har bir belgisi uchun $C_2=M*y^k \bmod q$ tenglikni hisoblash orqali shifrmatn olinadi, shifrlash amalga oshirilgach, k son o‘chirib tashlanadi va qabul qiluvchiga C_1,C_2 juftlik yuboriladi.

Shifrmatnni deshifrlash. Shifrmatn va maxfiy kalitga ega foydalanuvchi quyidagi ketma – ketliklarni bajarish orqali ochiq matnga ega bo‘ladi. Qabul qilingan ma’lumotlar asosida $M=C_1*C_2^{q-x-1} \bmod q$ ochiq matn hisoblanadi [12].

El-Gamal algoritmining gomomorfik xususiyati quyidagi teng bo‘ladi [1]:

$$E(m_1)\cdot E(m_2)=\left(g^{r_1},m_1\cdot h^{r_1}\right)\left(g^{r_2},m_2\cdot h^{r_2}\right)=$$
$$=\left(g^{r_1+r_2},(m_1\cdot m_2)\cdot h^{r_1+r_2}\right)=E(m_1\cdot m_2)$$

Paillier algoritmi. Algoritm birinchi marta Paskal Payet tomonidan taklif qilingan [11].

Kalitlarni hosil qilish.

1. Ikkita teng uzunlikdagi va $EKUB(pq,(p-1)(q-1))$ shartni qanoatlantiruvchi katta p va q tasodifiy tub sonlar generatsiya qilinadi;

2. $n=p\cdot q$ va $\lambda=lcm(p-1,q-1)$ bu yerda lcm bu eng kichik umumiy bo‘linuvchini hisoblaydi;

3. Tasodifiy $g\in Z_{n^2}^*$ butun g soni tanlanadi;

4. $\mu=\left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$ hisoblanadi, bu yerda $L(x)=\dfrac{x-1}{n}$;

5. Ochiq (shifrlash) kalit sifatida (n,g) olinadi;

6. Maxfiy (deshifrlash) kalit sifatida λ,μ olinadi.

Matnni shifrlash:

1. Shifrlash uchun $0<m<n$ shartni qanoatlantiruvchi m xabar olinadi;

2. Itiyoriy $o<r<n$ va $EKUB(r,n)=1$ shartni qanoatlantiruvchi r son hisoblanadi;

3. m xabar quyidagicha shifrlanadi: $c=g^m\cdot r^n \bmod n^2$.

Shifrmatnni deshifrlash

1. $c\in Z_{n^2}^*$ shifrmatn olinadi;

2. $m=L\left(c^{\lambda} \bmod n^2\right)\cdot\mu \bmod n.$

Paillier shifrlash algoritmi quyidagi gomomorfik xususiyatga ega:

$$D\left(E\left(g^{m_1},r_1^n\right)\cdot E\left(g^{m_2},r_2^n\right) \bmod n^2\right)=$$
$$=m_1+m_2 \bmod n$$

Ochiq matnlarning gomomorfik ko‘paytmasi

Shifrmatnni k o‘zgarmas songa ko‘paytirish natijasini deshifrlasak, shifrmatn va o‘zgarmas sonni ko‘pytmasiga teng bo‘ladi:

$$D\left((m_1,r_1)^k \bmod n^2\right)=km_1 \bmod n.$$

Goldvasser-Mikali shifrlash algoritmi. Goldwasser-Micali uchta algoritmdan iborat: ochiq va yopiq kalitni ishlab chiqaruvchi ehtimolli kalitlarni yaratish algoritmi, ehtimolli shifrlash algoritmi va deterministik deshifrlash algoritmi [11].

Sxema N ning faktorizatsiyasini (p,q) hisobga olgan holda x ning berilgan qiymati N

kvadrat modul ekanligini aniqlashga asoslangan. Buni quyidagi protsedura yordamida amalga oshirish mumkin:

1. $x_p = x \bmod p,\ x_q = x \bmod q$ qiymatlar hisoblanadi;

2. Agar $x_p^{(p-1)/2} \equiv 1 \bmod p$ va $x_q^{(q-1)/2} \equiv 1 \bmod q$ bo‘lsa, u holda x modul N bo‘yicha kvadratik chegirma bo‘ladi.

Kalitlarni hosil qilish.

1. Yetarlicha katta qiymatga ega p va q tub sonlari hosil qilinadi;

2. $N = p \cdot q$ hisoblanadi;

3. Yakobi simvoli $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$ shartini qanoatlantiruvchi, tasodifiy y son hosil qilinadi;

4. Topilgan (N, y) qiymatlar ochiq kalit sifatida olinadi, (p, q) sonlari yopiq kalit sifatida olnadi.

Matnni shifrlash.

Faraz qilinsin m xabar shifrlangan holda yuborilishi kerak bo‘lsin,

1. Dastlab m xabarni $m_1, m_2, ..., m_n$ ko‘rinishida ifodalab olinadi;

2. Har bir m_i bit uchun tasodifiy y_i qiymatlar hosil qilinadi, bunda $EKUB(y_i, N) = 1$ shart o‘rinli bo‘lishi kerak;

3. $c_i = y_i^2 x^{m_i} \bmod N$ ni hisoblash orqali $c_1, c_2, ..., c_n$ shifrmatnlar hosil qilinadi.

Shifrmatnni deshifrlash.

$c_1, c_2, ..., c_n$ shifrmatnlar to‘plamini deshifrlash quyidagicha amalga oshiriladi:

1. Har bir shifrmatnlar belgisi uchun (p, q) tub ko‘paytuvchilardan foydalanib, c_i shifrmatn kvadratik chegirma ekanligi tekshiriladi;

2. Agar c_i kvadratik chegirma bo‘lsa, u holda $m_i = 0$ aks holda $m_i = 1$ qiymat olinadi;

3. $m = (m_1, m_2, ..., m_n)$ shifrmatn olinadi.

Goldvasser-Mikali shifrlash algoritmda berilgan $r \in \{0, ..., m-1\}$ sonlari uchun ochiq kalit modul m va kvadratik qoldiq bo‘lmagan x dan iborat bo‘lsa, b bitni shifrlash funksiyasi $\varepsilon(b) = x^b r^2 \bmod n$ ga teng. Ushbu algoritm uchun gomomorfik xususiyat quyidagiga teng bo‘ladi:

$$E(b_1) \cdot E(b_2) = \left(x^{b_1} r_1^2 x^{b_2} r_2^2\right) =$$

$$= \left(x^{b_1+b_2} (r_1 r_2)^2\right) \bmod n = E(b_1 \oplus b_2)$$

Benahol algoritmi [7]:

Matnni shifrlash

$m \in Z_r$ xabarni shifrlash:

Ixtiyoriy $u \in Z_n^*$ son olinadi;

Keyin $E_r(m) = y^m u^r \bmod n$ shifrmatn hisoblanadi.

Shifrmatnni deshifrlash.

$c \in Z_n^*$ shifrmatnni hisoblash:

1. $a = c^{\phi/r} \bmod n$ hisoblanadi;

2. $m = \log_x(a)$ hisoblanadi. Bu yerda $x^m \equiv a \bmod n$.

Benaloh kriptotizimi qo‘shish operatsiyasiga nisbatan gomomorf:

$$E(m_1) \cdot E(m_2) = \left(g^{m_1} u_1^r\right)\left(g^{m_2} u_2^r\right) =$$

$$= g^{m_1+m_2} (u_1 u_2)^r = E(m_1 + m_2) \bmod r,$$

bu yerda $E(m)$, m xabarni shifrlash funksiyasi.

Umumiy qilib barcha qisman gomomorfik shifrlash algoritmlarini turli mezonlar bo‘yicha tavsiflash mumkin.

Qisman gomomorfik shifrlash algoritmlarining tavsifi 2- jadvalda keltirilgan [9].

Chegaralangan gomomorfik shifrlash (SWHE) faqat bir necha marta bajariladigan bir necha turdagi algebraik amallarni qo‘llab-quvvatlaydi. “Chegaralangan” gomomorfik shifrlash qo‘shish va ko‘paytirish gomomorfik amalini qo‘llashi bilan to‘liq va qisman shifrlashga qaraganda umumiyroqdir. Biroq, shifrlangan ma’lumotlarda faqat cheklangan miqdordagi amallarni bajarish mumkin [9]. Chegaralangan gomomorfik shifrlash sxemalari uchun Boneh-Goh-Nissim (BGN), GGH agoritmlarini misol qilish mumkin.

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

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 bo‘lishi talab qilingan.

2-jadval. Qisman gomomorfik shifrlash algoritmlari

Qisman gomomorfik shifrlash sxemalari	Shifrlash sxemalari						Gomomorfik shifrlash xossalari
	Simmetrik	Asssimmetrik	Ehtimoliy	Deterministik	Additive	Multiplikativ	Algoritm
RSA		+		+		+	$m_1^e \pmod n * m_2^e \pmod n = (m_1 * m_2)^e \pmod n$
Goldwasser-Mikali		+	+		+		$\left(y_1^2 x^{m_1} \pmod n\right) * \left(y_2^2 x^{m_2} \pmod n\right) = (y_1 * y_2)^2 x^{m_1+m_2} \pmod n$
El-Gamal		+	+			+	$E(m_1) \cdot \varepsilon(m_2) = \left(g^{r_1}, m_1 \cdot h^{r_1}\right)\left(g^{r_2}, m_2 \cdot h^{r_2}\right) = \left(g^{r_1+r_2}, (m_1 \cdot m_2) h^{r_1+r_2}\right) = E(x_1 x_2)$
Benahol		+	+		+		$\left(y^{m_1} u_1^r \pmod n\right) * \left(y^{m_2} u_2^r \pmod n\right) * * \left(y^{m_2} u_2^r \pmod n\right) = y^{m_1+m_2} (u_1 * u_2)^n \bmod n$
Paillier		+	+		+		$\left(\left(g^{m_1} r_1^n\right) \pmod{n^2}\right) * \left(\left(g^{m_2} r_2^n\right) \pmod{n^2}\right) = y^{m_1+m_2} (r_1 * r_2)^n \bmod n^2$
Naccache-Stern		+	+	+	+		$E(m_1) \times E(m_2) = \left(g^{m_1} \times r_1^\sigma\right)\left(g^{m_2} \times r_2^\sigma\right) \bmod n = g^{m_1+m_2} \times (r_1 \times r_2)^\sigma \pmod n = E(m_1 + m_2) \bmod n$
Damgard-Jurik		+	+		+		$E_{s,g}(m_1, u_1) \times E_{s,g}(m_2, u_2) = \left(g^{m_1} \times (u_1)^{n^s}\right) \times \left(g^{m2} \times (u_2)^{n^s}\right) \bmod n^{s+1} = g^{m_1+m_2} \times (u_1 \times u_2)^{n^s} \bmod n^{s+1} = E_{s,g}(m_1 + m_2, u_1 \times u_2) \bmod n^{s+1}$
Okamoto Uchiyama		+	+		+		$E_g(m_1, r_1) \times E_g(m_2, r_2) = \left(g^{m_1} \times h^{r_1}\right) \times \left(g^{m_2} \times h^{r_2}\right) \bmod n = g^{m_1+m_2} \times h^{r_1+r_2} \bmod n = E_g(m_1 + m_2, r_1 \times r_2) \bmod n$

Kalitlarni hosil qilish. Xavfsizlik parametrlarini kiritishda q_1 va q_2 ehtimollik boshlang‘ich qiymatlar, $n = q_1 \cdot q_2$ tartibli G, G_T guruhlar va e ikki chiziqli akslantirish bo‘lib, $e: G \times G \to G_1$ tanlanadi. Bu yerda, $G, G_1, n = q_1 \cdot q_2$ ga teng qiymatlar. G guruhga tegishli g, u qiymatlar tanlanadi va $h = u^{q_2}$ hisoblanadi. Ochiq kalit sifatida $p_k = (n, G, G_T, e, g, h)$ olinadi va maxfiy kalit sifatida $s_k = q_1$ olinadi.

Xabarni shifrlash. Ochiq kalit p_k va $m \in M$ xabar berilgan bo‘lsin, tasodifiy $r \in_R Z_n$ soni tanlanadi va shifrmatn hisoblanadi:

$$c = g^m h^r \bmod n.$$

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

$c^{q_1} = \left(g^m h^r\right)^{q_1} = \left(g^{q_1}\right)^m \left(u^n\right)^r = \left(g^{q_1}\right)^m$ va xabarlar fazosi polynomial 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 chegaralangan 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:

$$c_1 \cdot c_2 \cdot h^r = g^{m_1} \cdot h^{r_1} \cdot g^{m_2} \cdot h^{r_2} \cdot h^r = \\ = g^{m_1+m_2} h^{r_1+r_2+r} = g^{m_1+m_2} h^{r'}.$$

Bu haqiqatan ham $(m_1 + m_2) \bmod n$ xabari uchun c haqiqiy BGN shifrmatn ekanligini anglatadi, bu erda $r' = (r_1 + r_2 + r') \bmod n$ tasodifiy butun sondir.

Ko‘paytirish. Shifrlangan xabarlarni gomomorf tarzda ko‘paytirish uchun qo‘shimcha kuzatishlar kerak bo‘ladi. $e(g,g) = g_1$ tartibi n bo‘lgan G_T guruhning bir generatori va $e(g,h) = h_1$ esa G_T guruhning boshqa bir elementi bo‘lsin. Ta’kidlash lozimki $e(g,h) = e\left(g, u^{q_2}\right) = e(g,u)^{q_2} = h'^{q_2} = h_1$. G_T guruhning tartibi $n = q_1 \cdot q_2$ ekanligidan h_1 elementi h_2 tartibida bo‘lishi kerak. Qo‘shimcha ravishda biron bir $a \in Z$ uchun $h = g^{aq_2}$ deb belgilab olamiz. Endi sozlama yuqoridagidek bo‘lsin. Ixtiroriy $r \in Z_n$ son tanlanadi va $c = e(c_1, c_2) \cdot e(g,h)^r$ hisoblanadi, bu ikki chiziqlilikdan foydalanish orqali

$$c = e(c_1, c_2) \cdot e(g,h)^r = e\left(g^{m_1} h^{r_1}, g^{m_2} h^{r_2}\right) h_1^r = \\ = e\left(g^{m_1}, g^{m_2} h^{r_2}\right) \cdot e\left(h^{r_1}, g^{m_2} h^{r_2}\right) \cdot h_1^r = \\ e\left(g^{m_1}, g^{r_1}\right) \cdot e\left(g^{m_2}, g^{r_2}\right) \cdot e\left(h^{r_1}, h^{r_2}\right) \cdot h_1^r = \\ = g_1^{m_1 m_2} h_1^{m_1 r_2} h_1^{m_2 r_1} h_1^{aq_2 r_1 r_2} h_1^r = \\ = g_1^{m_1 m_2} h_1^{m_1 r_2 + m_1 r_2 + q_2 r_1 r_2 + r} = g_1^{m_1 m_2} h_1^{r'}$$

shifrmatn hisoblanadi.

Bu haqiqatan ham $(m_1 + m_2) \bmod n$ xabari uchun c haqiqiy BGN shifrmatn ekanligini anglatadi, $r' = (m_1 r_2 + m_2 r_1 + q_2 r_1 r_2 + r) \bmod n$ miqdor Z_n to‘plamning elementlari va h_1 element q_1 tartibli bo‘lganligi uchun $\left(h_1^{r'}\right)^{q_1} = \\ = \left(h_1^{q_1}\right)^{r'} = 1 \in G_T$ munosabat o‘rinli bo‘lib deshifrlash amalga oshadi.

Ko‘paytirishdan keyingi qo‘shish amali. Shifrlangan ma’lumotlar ustida ko‘paytirish amalidan keyin ham gomomorfik qo‘shish amalini bajarish mumkin. Agar G_T da shifrlangan matnlarni olish kerak bo‘lsa, $c^* = g_1^{m^*} h_1^{r^*}$ ni hisoblash orqali G_T da m' xabarining shifrlanishini to‘g‘ridan-to‘g‘ri taqdim etish orqali shifrlangan matn hosil qilish mumkin. G_T to‘plamda c_1 va c_2 shifrmatnlarni qo‘shishda yangi tasodifiy $r \in_R Z_n$ tanlanadi va quyidagi hisoblanadi:

$$c_1 \cdot c_2 \cdot h_1^r = g_1^{m_1} h_1^{r_1} g_1^{m_2} h_1^{r_2} h_1^r = \\ = g_1^{m_1+m_2} h_1^{r_1+r_2+r} = g_1^{m_1+m_2} h_1^{r'}.$$

Bu haqiqatan ham $(m_1 + m_2) \bmod n$ xabari uchun c haqiqiy BGN shifrmatn ekanligini anglatadi, bu erda $r' = (r_1 + r_2 + r) \bmod n$ tasodifiy butun sondir.

Ushbu qisman gomomorfik shifrlash algoritmlarining bardoshliligi ularni tashkil etgan kriptografik algoritmlarning matematik muammolari bilan bevosita bog‘liq. Amaldagi qisman gomomorfik shifrlash algoritmlari katta sonlarni tub ko‘paytuvchilarga ajratish, chekli maydonda sonlarni diskret logarifmlash va chekli maydonda elliptk egri chiziqlarning ratsional nuqtalarini aniqlash muammosiga asoslanadi. Chekli maydonda elliptk egri chiziqlarning ratsional nuqtalarini aniqlash muammosiga asoslangan BGN kriptotizimi ochiq matn ustiga chegaralangan ikkita qo‘shish va ko‘paytirish arifmetik amal bajarishi bilan samaraliroq hisoblanadi.

To‘liq gomomorfik shifrlash. To‘liq gomomorf shifrlash sxemasi shifrlangan ma’lumotlarda cheksiz miqdordagi additiv va multiplikativ gomomorfik amallarni bajarish imkoniyatiga ega [9].

To‘liq gomomorf shifrlash sxemalari asosan to‘rtta matematik muammolarga asoslangan toifalarga bo‘lish mumkin:

1. **Ideal panjara** muammosi asosiga asoslangan;
2. **Butun sonlarga** asoslangan;
3. **Xato bilan o‘rganish (LWE)** muammosiga asoslangan;
4. **NTRU** asosidagi sxemalariga asoslangan.

Panjaralar. Ta’rif: R^m bu m o‘lchamli Yevklid fazosi bo‘lsin va R^m fazoda bir-biridan mustaqil n ta $b_1,...,b_n$ vektorlar berilgan bo‘lsin, $(m \geq n)$.

Quyida R^m fazoda berilgan ifoda panjara sifatida ta’riflanadi:

$$L(b_1,...,b_n) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in Z \right\}. \qquad (1)$$

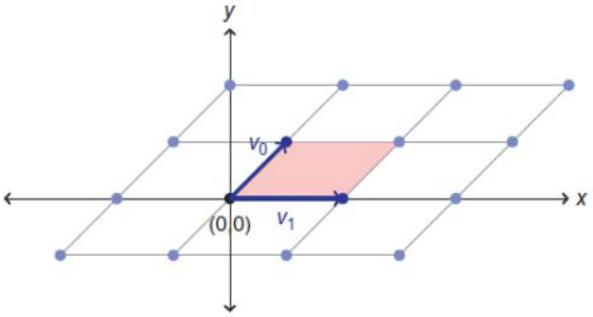
Panjaraning o‘lchami m va panjara darajasi n deb olib, $m = n$ bo‘lganda ya’ni bazis vektorlari koordinatalar soniga teng bo‘lsa, uni to‘liq darajali yoki to‘liq o‘lchovli panjara deb ataladi. Panjara asosi bu $b_1,...,b_n$ vektorlar ketma-ketligi hisoblanadi va u qulay tarzda matritsa sifatida ifodalanadi:

$$B = [b_1,...,b_n] \in R^{m \times n}. \qquad (2)$$

(1) ifodani (2) matritsa va vektor matritsadan foydalanib, quyidagicha yozish mumkin:

$$L(B) = \left\{ Bx : x \in Z^n \right\}. \qquad (3)$$

Grafik jihatdan, n o‘lchovli cheksiz muntazam to‘rda panjara - bu to‘rning kesishish nuqtalari to‘plami hisoblanadi. To‘r ortogonal bo‘lishi shart emas. 5-rasmda 2 o‘lchamli panjaraga misol ketirilgan [9].



5-rasm. R^2 fazoda ikki o‘lchamli panjara

Panjara asosi yagona emas. Panjara turli xil asoslarga ega bo‘lishi mumkin. Agar asos vektorlari deyarli ortogonal bo‘lsa, uni “yaxshi” asos deb ataladi. Aks holda, u “yomon” asos deb ataladi. Odatda, “yomon” asoslar “yaxshi” asoslarga qaraganda qisqaroq.

Eng qisqa vector muammosi (SVP) muammosi asosini hisobga olgan holda panjaradagi nolga teng bo‘lmagan eng qisqa vektorni topadi.

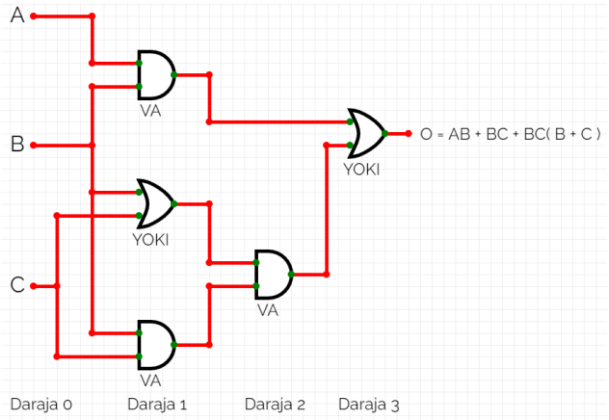
Ta’rif**:** (*Eng qisqa vector muammosi, SVP*). $B \in^{m \times n}$ ixtiyoriy bazis vektor berilgan bo‘lsin, u holda ixtiyoriy $y \in Z^n \{0\}$ qiymatlar uchun $\|Bx\| \leq \|By\|$ shartni qanoatlantiruvchi nolga teng bo‘lmagan $Bx\left(x \in Z^n\right)$ panjara vektorini topish eng qisqa vektor muammosi deyiladi.

Eng yaqin vektor muammosi (CVP) muammosi, panjaraning berilgan nuqtasiga eng yaqin panjara nuqtasini topadi.

Ta’rif**:** (*Eng yaqin vektor muammosi CVP*). $B \in Z^{m \times n}$ ixtiyoriy bazis vektori bo‘lsin. Ixtiyoriy $y \in Z^m$ uchun eng qisqa butun $x \in Z^n$ vektorni topish quyidagicha ifodalanadi $\|Bx - t\| \leq \|By - t\|$ va bu ifoda $t \in Z^m$ maqsad vektorisa eng yaqin bo‘lgan Bx panjara vektorini topish muammosi deyiladi [9].

Sxemalar. Sxemalar yo‘naltirilgan va asiklik grafiklar bo‘lib, bu yerda tugunlar *eshiklar* deb ataladi va chekkalari *simlar* deb ataladi. Sxemaning kirish qiymatlari butun sonlar, mantiqiy qiymatlardir. Tegishli eshiklar o‘rnatilgan operatsiyalar va arifmetik amallar yoki mantiqiy kirishlar hisoblanadi. F funktsiyasini baholash uchun f sxema sifatida ifodalanadi va uning eshiklarini topologik jihatdan ketma-ket bajariladigan darajalarga joylashtiriladi.

Faraz qilaylik, kirish qiymatlari (A,B,C) bo‘lgan f funksiya quyidagi ifodani chiqaradi**:** $A \cdot B + B \cdot C \cdot (B + C)$**.** Quyidagi 6-rasmda f funksiyani mantiqiy eshiklari *AND* va *OR* bilan ifodalangan [13].



6-rasm. Mantiqiy sxemani tasvirlash grafigi

Sxemalar uchun murakkablikning ikkita muhim mezoni - bu *o'lcham* va *chuqurlikdir*.

C sxemasining *o'lchami* uning kirish bo'lmagan tugunlari sonidir. C sxemasining *chuqurligi* uning kirish tugunidan chiqish tugunigacha bo'lgan eng uzun yo'lining uzunligi, uning asosiy yo'naltirilgan grafigidir [2].

1. Ideal panjaraga asoslangan to'liq gomomorfik shifrlash sxemasi.

Kreyg Gentry [10] ixtiyoriy chuqurlikdagi sxemalarda amallar bajarishi mumkin bo'lgan birinchi shifrlash sxemasini taqdim etdi. Ushbu protsedura to'liq gomomorf bo'lmagan sxemani to'liq gomomorf sxemaga aylantirish uchun ishlatilishi mumkin.

Taklif etilgan shifrlash sxemasi uchta asosiy bosqichdan iborat:

1-qadam. Ideal panjaralar asosida Chegaralangan gomomorfik shifrlash (SWHE) sxemasini qurish**.**

Chegaralangan shifrlash sxemasi algoritmlari:

Kalitlarni hosil qilish algoritmi. Xabarni shovqin vektoriga joylashtirish uchun kirish sifatida o'rnatilgan R halqasini va kichik ideal $I \in R$ ning asosi B_I ni oladi. Bundan tashqari $IdealGen(R, B_I)$ algoritmi bilan kalitlar generatsiya qilinadi. Ideal panjara J ning "yaxshi" B^{sk} bazisi maxfiy kalit tuchun ishlatiladi. Ideal panjara J ning "yomon" B^{pk} bazisi ochiq kalit tuchun ishlatiladi. Ideal panjara J shuningdek I, R qiymatlar o'zaro tub va ular uchun $I + R = J$ o'rinli.

$Samp()$ algoritmi shifrlash algoritmida idealni panjarani ma'lum bir miqdorni siljitish orqali ideal panjaradan qisqa vector andozasini olish uchun ishlatiladi.

Ochiq kalitlar sifatida $\left(R, B_I B_J^{pk}, Samp(\ )\right)$ olinadi va maxfiy kalit sifatida esa, B_J^{sk} olinadi.

Shifrlash algoritmi. Ochiq kalit B^{pk} va m xabar olinadi. Ochiq matnlar fazosi P, $R(\bmod B_J)$ to'plamning qism to'plami hisoblanadi.

$Samp(\vec{m}, B_i)$ algoritmidan foydalanib, $\vec{e} = \vec{m} + \vec{i}$ vektorini tanlab olish uchun B_j^{pk} umumiy bazis moduliga qisqartiriladi

$$E(\vec{m}) = \vec{e}\left(\bmod B_j^{pk}\right) = \left(\vec{m} + \vec{i}\right)\left(\bmod B_j^{pk}\right) = \vec{c}.$$

Bu holda shifrlangan matn vektor $\vec{c}$ bo'lib, u eng yaqin panjara nuqtasigacha bo'lgan masofada kodlangan.

Gomomorfik amallar. B_j^{pk} ochiq kalit, $\psi = \{\vec{c}_1, ..., \vec{c}_2\}$ ruxsat etilgan C gomomorfik sxemalar to'plamidan B_I moduli bo'yicha operatsiyalariga ega C sxemasi olinadi. Gomomorfik amallar orqali hosil bo'lgan shifrmatn c ni hisoblash uchun gomomorfik qo'shish Add_{BI} va gomomorfik ko'paytirish $Mult_{BI}$ amallari ma'lum ketma-ketlikda bajariladi.

$Add\left(B_J^{pk}, \vec{c}_1, \vec{c}_2\right)$ natija $\vec{c}_1 + \vec{c}_2\left(\bmod B_J^{pk}\right)$,

$Mult\left(B_J^{pk}, \vec{c}_1, \vec{c}_2\right)$ natija $\vec{c}_1 \cdot \vec{c}_2\left(\bmod B_J^{pk}\right)$.

Shifrmatnni hisoblash jarayonida algoritm ochiq matnlarga $\bmod B_I$ bo'yicha C sxemasini qo'llaydi, so'ngra C sxemaning Add_{BI} va $Mult_{BI}$ operatsiyalarini R halqasida qo'shish + va ko'paytirish * halqa operatsiyalari bilan almashtiradi.

Deshifrlash algoritmi:

$$\vec{m} = \left(\vec{c}\left(\bmod B_j^{sk}\right)\right) \bmod B_I = \vec{e}\left(\bmod B_I\right).$$

Chunki, $\vec{e} = \vec{m} + \vec{i}$ va bu yerda $\vec{i} \in I$.

Shovqin parametri panjara nuqtasiga juda yaqin bo'lsa, shifrlangan matnda ko'proq qo'shish

va ko‘paytirish qo‘llanilishi mumkin. Chegara nuqtasidan keyin shifrlangan matnni to‘g‘ri deshifrlash imkoni yo‘q. Har bir “qo‘shish” amali bilan shovqin parametri chiziqli ravishda o‘sib boradi va har bir “ko‘paytirish” amali bilan shovqin eksponent ravishda o‘sadi. Ko‘paytirish amallari bilan shovqin tezroq oshadi, shuning uchun gomomorfik amal bajarishda ko‘paytirish operatsiyalari soni cheklangan bo‘ladi.

2-qadam. Squashing (Soddalashtirish). Deshifrlash sxemasini soddalashtirish uchun ochiq kalitga maxfiy kalit haqida ishora beriladi. Bu ba’zi hisob-kitoblarni deshifrlash bosqichidan shifrlash bosqichiga o‘tkazadi. Biroq, bu protsedura dastlabki sxemaning xavfsizligini zaiflashtiradi. Maxfiy kalitni tiklashning zaifligini bartaraf etish uchun kam to‘plamlar yig‘indisi muammosidan (SSSP) foydalaniladi.

Soddalashtirish protsedurasi deshifrlash algoritmini ikki bosqichga ajraladi:

- Shifrlovchi dastlabki hisoblash yo‘li bilan intensiv qayta ishlash bosqichini maxfiy kalitsiz amalga oshiradi;
- Deshifrlovchi maxfiy kalitdan foydalanib, yengil hisoblash bosqichini amalga oshiradi.

3-qadam. **Bootstrapping.** Agar deshifrlash algoritmi gomomorfik sxemani amlaga oshira olsa, bunday sxema bootstraping qilish imkoniga ega deb ataladi. Bootstrapping asosan shifrlangan matnda gomomorf amallarni bajargandan so‘ng shovqinni kamaytirish uchun “yangilash” protsedurasidir. Buni amalga oshirish uchun avval (pk_1, sk_1) va (pk_2, sk_2) kalit juftlari yaratiladi. Keyin, m xabar birinchi ochiq kalit pk_1 bilan $c = E_{pk_1}(c) = \left(E_{pk_1}(m)\right)$ kabi shifrlanadi, yana c shifrmatn ikkinchi ochiq kalit pk_2 bilan shifrlanadi ya’ni $E_{pk_2}(c) = E_{pk_2}\left(E_{pk_1}(m)\right)$ amalga oshiriladi va birinchi maxfiy kalit ikkinchi ochiq kalit bilan shifrlanadi, ya’ni, $E_{pk_2}(sk_1)$. Keyin bulut provayderiga $E_{pk_2}(sk_1)$ va $E_{pk_2}(c)$ matnlar uzatiladi. Soddalashtirilgan chegaralangan gomomorfik shifrlash sxemasi o‘zining deshifrlash halqasida gomomorfik amal bajarganligidan, bulut provayderi dastlabki ikkinchi ochiq kalit bilan shifrlangan dastlabki maxfiy kalit sk_1 ostida shifrlangan ya’ni $E_{sk_2}(sk_1)$ dan foydalanib gomomorfik shovqinli shifrmatn uchun deshifrlash sxemasini qo‘llay oladi. Shuning uchun $E_{pk_2}\left(D_{sk_1}(c)\right) = E_{pk_2}(m)$, bunda shifrmatn mijoz tomonidan ikkinchi maxfiy kalit sk_2 dan foydalanib deshifrlanadi, ya’ni $D_{sk_1} = \left(E_{pk_1}(m)\right) = m$ [9].

2. Butun sonlarga asoslangan to‘liq gomomorfik shifrlash sxemalari.

Sxema taxminiy eng katta umumiy bo‘luvchi (AGCD) muammosiga asoslangan. AGCD muammosi $x_i = pq_i + r_i$ to‘plamidan p ni topishga asoslangan.

Sxema Gentrining ideal panjara sxemasidan kontseptual jihatdan sodda, ammo gomomorf operatsiyalar va samaradorlik bo‘yicha o‘xshash xususiyatlarga ega. Taklif etilayotgan simmetrik SWHE sxemasi quyidagicha tasvirlangan.

Kalitlarni hosil qilish algoritmi. Biron berilgan $p \in \left[2^{\eta-1}, 2^{\eta}\right]$ oraliqdan p toq son kalit sifatida olinadi.

Shifrlash algoritmi. $m \in \{0,1\}$ xabar bitlarini shifrlash quyidagicha amalga oshiriladi: $E(m) = m + 2r + pq = c$ bu yerda r, q tasodifiy sonlar va $r < p/2$.

Deshifrlash algoritmi.

$$D(c) = \left(c(\bmod p)\right) \bmod 2 = m.$$

Gomomorfik amallar. Berilgan (ikkilik) sxema butun sonlar ustida barcha amallarni bajaradi va natijada olingan butun sonni qaytaradi.

Gomomorfik qo‘shish amali:

$$c_1 + c_2 = E(m_1) + E(m_2) =$$
$$= m_1 + 2r_1 + pq_1 + m_2 + 2r_2 + pq_2 = (m_1 + m_2) +$$
$$+2(r_1 + r_2) + (q_1 + q_2)p = E(m_1 + m_2).$$

Agar shovqin uchun $r_1 + r_2 < p/2$ munosabat o‘rinli bo‘lsa, u holda $E(m_1 + m_2)$ shifrmatn deshifrlanadi.

Gomomorfik ko‘paytirish amali:

$$c_1 c_2 = E(m_1)E(m_2) =$$
$$= (m_1 + 2r_1 + pq_1)(m_1 + 2r_1 + pq_1) =$$
$$= m_1 m_2 + 2(m_1 r_2 + m_2 r_1 + 2r_1 r_2) +$$
$$+(pq_1 q_2 + 2q_1 r_2 + m_1 q_2 + 2q_2 r_1 + m + 2q + 1)p =$$
$$= E(m_1 m_2).$$

Agar shovqin uchun $2r_1 r_2 + m_1 r_2 + m_2 r_1 < p/2$ o‘rinli bo‘lsa, u holda shifrmatn deshifrlanadi.

Sxema qo‘shishga qaraganda kamroq gomomorf ko‘paytirish operatsiyalarini bajaradi, chunki shovqin ko‘paytirish operatsiyasi bilan eksponent ravishda o‘sadi:

$$r_1 + r_2 < \frac{p}{2} \quad 2r_1 r_2 + m_1 r_2 + m_2 r_1 < \frac{p}{2}.$$

Ushbu chegaralangan gomomorfik shifrlash sxemasini to‘liq gomomorfik shifrlash sxemasiga

aylantirish uchun Dijk va boshqalar kabi soddalashtirish (squashing) va yuklash (bootstrapping) usullaridan foydalangan [16].

3. Xatolar bilan o‘rganish (LWE)ga asoslangan to‘liq gomomorfik shifrlash sxemalari.

Brakerski va Vaikuntanathan amaliy to‘liq gomomorfik shifrlash sxemasi yo‘lida ajoyib yaxshilanishga erishdilar. Ular polinomial-xatolar bilan o‘rganish (PLWE) ga asoslangan yangi chegaralangan gomomorfik shifrlash sxemasini taqdim etdilar. Polinomial-xatolar bilan o‘rganish, o‘z navbatida, halqa xatolar bilan o‘rganishning oddiy versiyasi bo‘lib, ular ikkita usuldan, ya'ni Gentryning to‘liq gomomorfik shifrlash sxemasiga erishishga qaratilgan soddalashtirish (squashing) va yuklash (bootstrapping) usulidan foydalanganlar [9].

Kalitlarni hosil qilish algoritmi.

1. p tub soni va q butun soni tanlanadi $q > p^2$;

2. n musbat butun son olinadi va tasodifiy $A \in Z_q^{(n\times m)}$ matritsa, tasodifiy s, e vektorlar va $u \in Z_q^n$ tanlab olinadi;

3. $b = (A, As + e)$ qiymat va $B = (b \mid u)$ matritsa hisoblanadi;

4. Ochiq kalitlar sifatida (A, B) olinadi va maxfiy kalit sir saqlanadi.

Shifrlash algoritmi. Xabar fazosi ikkilik koeffitsientli polinomlarning halqasidir $R_2 = \dfrac{z_2[x]}{(x^n+1)}$ Ya’ni, xabar Z_2 koeffitsientlari bilan n da1rajali polinom sifatida kodlangan. Shifrlash uchun, namuna $a, b = (as + 2e) \in R_q^2$, bu yerda $a \leftarrow R_q$ va $e \leftarrow \chi, c_0 = b + m \in R_q$.

E’tiborli jihati shundaki, shifrlovchi orqali (a, b) namunalarni olish uchun faqat s kalit foydalaniladi.

Deshifrlash algoritmi. Bizga $c = (c_0 c_1)$ shifrmatnlar berilgan bo‘lsin va bu shifrmatnlarni deshifrlash qudidagicha amalga oshiriladi:

$$c_0 + c_1 s \pmod 2.$$

Gomomorfik amallar. Quyida R_2 da ikkita elementni gomomorf tarzda qo‘shish va ko‘paytirish usuli keltiriladi.

Gomomorfik qo‘shish amali. Ikkita shifrmatnlar berilgan bo‘lsin. $c = (c_0, c_1)$ va $c' = (c_0', c_1')$.

$$c_{add} = c + c' = E(m) + E(m') =$$
$$= (c_0, c_{1'}) + (c_0', c_1') = (c_0 + c_0', c_1 + c_1') =$$
$$= (as + 2e + m, -a) + (a's + m', -a') =$$
$$= ((a + a')s + 2(e + e') + (m + m'), -(a + a')) =$$
$$= E(m + m').$$

Asosiy xabarlar yig‘indisi shifrlangan matn vektorlariga vektor qo‘shishni qo‘llash orqali olinadi va shovqinni kichik darajada ushlab turadi.

Gomomorfik ko‘paytirish amali. Multiplikativ gomomorfizm bilan shug‘ullanish uchun ehtiyot bo‘lish kerak. Ikkita xabar ishlab chiqarishdan olingan elementni yaratish uchun ikkita shifrlangan matnning c_0 elementlarini ko‘paytirish kerak. Ikkita $c = c_0 c_1$ va $c' = (c_0', c_1')$ shifrmatnlar berilgan bo‘lsin. U holda, shifrlangan ma’lumotlarning gomomorfik ko‘paytmasi quyidagicha hisoblanadi:

$$c_0 c_0' = -aa's^2 + (c_0 a' + c_0' a)s +$$
$$+2(2ee' + em' + e'm) + mm'.$$

Natijaviy shifrmatn esa quyidagicha bo‘ladi $c_{mult} = (c_{mult,o} c_{mult,1} c_{mult,2})$ yerda $c_{mult,2} = c_1 c_1'$, $c_{mult,1} = c_0 c_1' + c_0 c_1$, $c_{mult,0} = c_0 c_0'$. Shu ma’lumki, $m + 2e = c_0 + c_1 s$ va $m' + 2e' = c_0' + c_1' s$ ekanligidan quyidagi o‘rinli bo‘ladi:

$$(m + 2e) \cdot (m' + 2e') = (c_0 + c_1 s)(c_0' + c_1' s).$$

Shunday qilib, c_{mult} shifrmatnni hisoblash mumkin:

$$(c_0 + c_1 s)(c_0' + c_1' s) =$$
$$= c_{mult,0} + c_{mult,1} s + c_{mult,2} s^2.$$

Deshifrlanuvchi shifrma’lumot 3 ta $c = (c_0, c_1, c_2)$ elementni o‘z ichiga oladi va quyidagi bajariladi:

$$m = c_0 + c_1 s + c_2 s^2 \pmod 2.$$

Gentri LWE ga asoslangan BGN tipidagi kriptotizimni taklif qildi. Shundan so‘ng, Brakerski va Vaikuntanathan standart LWE muammolariga asoslangan boshqa SWHE sxemasini taqdim etdilar, bu erda ular qayta chiziqli ishlov berishni amalga oshirdilar [17].

4. NTRU sxemasiga asoslangan to‘liq gomomorfik shifrlash sxemasi.

N-daraja Kesilgan polinom (NTRU) ochiq kalitli kriptotizim bo‘lib, panjaradagi eng qisqa vektor muammosiga (SVP) asoslangan. Shifrlash jarayoni xabarni polinomga kodlashni va keyin unga shovqin qo‘shishni o‘z ichiga oladi. Shifrni ochish jarayoni ma'lum bir me'yorda shifrlangan

matnli ko‘phadga eng yaqin ko‘phadni topish orqali xabarni tiklashni o‘z ichiga oladi [4].

Kalitlarni hosil qilish algoritmi:

1. N, p, q butun sonlari tanlanadi bu yerda p va q sonlar $p \cdot q \bmod 2N = 1$ a mos keladigan katta tub sonlar va p soni $q-1$ ning bo‘luvchisi;

2. $\{-1,0,1\}$ to‘plamda koeffitsientlarga ega $N-1$ darajali tasodifiy $f(x)$ polinom hosil qilinadi;

3. Ko‘phadning q modul bo‘yicha teskarisi hisoblanadi $f^{-1}(x) \bmod q$;

4. Kichik e butun soni tanlanadi va $g(x) = (1 + f(x))^e \bmod p$ hisoblanadi;

5. Ochiq kalit sifatida $(p, q, g(x))$ va yopiq kalit sifatida $(f(x), f^{-1}(x))$ olinadi.

Shifrlash algoritmi:

1. m ochiq matn xabari $\{-1,0,1\}$ to‘plamda koeffitsientlarga ega darajali $m(x)$ ko‘pxadga kodlanadi;

2. Kichik butun r soni tanlanadi va $h(x) = rg(x) + m(x)$ modq hisoblanadi;

3. Shifrmatn sifatida $c = h(x)$ olinadi.

Deshifrlash algoritmi:

1. $c(x) = h(x) * f^{-1}(x) \bmod q$ hisoblanadi;

2. $m(x) = round(c(x) \bmod p) \bmod 2$ hisoblanadi, bu yerda $round(\ )$ butun songa yaqin sonni hisoblash funksiyasi;

3. Deshifrlangan matn $m(x)$ polinomial matn ko‘rinishida bo‘ladi.

Gomomorfik amallar.

Gomomorfik qo‘shish amali. Ikkita $h_1(x)$ va $h_2(x)$ shifrmatnlar berilgan bo‘lsa, gomomorfik qo‘shish quyidagicha amalga oshadi:

$$h_3(x) = h_1(x) f^{(-1)}(x) + h_2(x) f^{(-1)}(x) =$$
$$= (r_1 g_1(x) + m_1(x)) + (r_1 g_1(x) + m_2(x)) =$$
$$= g_1(x) + r_2 g_1(x)) + ((m_1(x) + m_2(x)) =$$
$$= (r_1(1 + f_1(x)) + r_2(1 + f_2(x))) +$$
$$+ (m_1(x) + m_2(x)) =$$
$$= (r_1 + r_2 + f_1(x) * f^{(-1)}(x) + f_2(x) *$$
$$* f^{(-1)}(x) + (m_1(x) + m_2(x)) =$$
$$= (r_1 + r_2 + m_1(x) + m_2(x) = m_1(x) + m_2(x).$$

Bu yerda shifrmatn $m(x) = m_1(x) + m_2(x)$ polinomial matn ko‘rinishida bo‘ladi.

Gomomorfik ko‘paytirish amali. (Bootstrapping):

1. $h(x)$ shifrmatn $c(x) = h(x) * f^{-1}(x)$ orqali shifrlanadi deshifrlanadi;

2. Z_p to‘plamga tegishli a tasodifiy son tanlanadi;

3. $c'(x) = (c(x) + a * f(x)) mod\ q$ hisoblanadi;

4. $m'(x) = round(c'(x) mod\ p) mod 2$ hisoblanadi;

5. $h'(x) = 2r * (g(x)^a) mod\ q$ hisoblanadi;

6. $h''(x) = h(x) - h'(x) mod\ q$ hisoblanadi;

7. $h3(x) = h''(x) + h'(x) * m'(x) mod\ q$ hisoblanadi;

8. Shifrlangan natija $(h3(x))$ shifrmatn ko‘rinishida bo‘ladi.

Yuqoridagi bootstrapping bosqichi chuqurroq gomomorfik sxemalari uchun bir necha marta takrorlanishi mumkin. Ushbu sxemalarning to‘liq gomomorfik jihati NTRU kriptotizimining chegaralangna gomomorfik shifrlash sxemasi ekanligidan kelib chiqadi. Bu shuni anglatadiki, ikkita shifrlangan matn qo‘shilishi natijasida mos keladigan ochiq matnlar yig‘indisiga shifrlash mumkin bo‘lgan shifrlangan matn paydo bo‘ladi [4].

Biroq, NTRUga soslangan kriptotizimlarda shifrlangan matnlarni ko‘paytirish bevosita mumkin emas. Shuning uchunu sxemalar gomomorf ko‘paytirishni amalga oshirish uchun yuklash (bootstrapping) texnikasidan foydalanadi. Deyarli barcha gomomorfik shifrlash sxemalari yuqoridagi 4 ta toifadagi usullardan kelib chiqib rivojlanib kelmoqda.

Gomomorfik shifrlash algoritmlariga asoslangan ilovalar. Gomomorfik shifrlash algoritmlariga oid bir qancha ilovalar, kutubxonalar va kompilyatorlar ishlab chiqilgan [14].

To‘liq gomomorfik shifrlash kutubxonalarining asosiy maqsadi To‘liq gomomorfik shifrlash sxemasi amallarini API orqali amalga oshirishdir. $KeyGen, Enc, Dec$ va $Eval$ tomonidan taqdim etilgan asosiy funksionallikdan tashqari, keng tarqalgan kutubxonalarning aksariyati shifrlangan matnni saqlash va manipulyatsiya, shuningdek, gomomorf qo‘shish va ko‘paytirish usullarini ta’minlaydigan qo‘shimcha funktsiyalarni o‘z ichiga oladi.

Ilk nashr etilgan kutubxona Halevi va Shoup tomonidan HElib (Gomomorf shifrlash kutubxonasi) bo‘lib, u C++ da amalga oshirilgan va NTL kutubxonasi ustiga qurilgan. Bundan tashqari, Microsoft SEAL, TFHE, PALISADE, TenSEAL, Lattigo, HEAAN kabi kutubxonalar mavjud.

Mavjud ochiq manba to‘liq gomomorfik shifrlash kutubxonalari, ular yozilgan til, qo‘llab-quvvatlanadigan to‘liq gomomorfik shifrlash sxemalari va oxirgi yangilanish sanasi 3-jadvalda keltirilgan [14].

3-jadval. Gomomorfik shifrlash algoritmlari kutubxonalari

Kutubxona	Til	Gomomorfik shifrlash sxemalari					Ishlab chiqaruvchilar	Oxirgi yangilangan sanasi
		BGV	B/VF	FHEW	TFHE	CKKS		
Helib	C++	+	-	-	-	+	IBM	1/10/2021
Microsoft SEAL	C++/C#	+	+	-	-	+	Microsoft	24/3/2022
PALISADE	C++	+	+	+	+	+	Duality Technologies	30/4/2022
Lattigo	Go	-	+	-	-	+	EPFL-LDS, Tune Insight	13/6/2022
FHEW	C++	-	-	+	-	-	Leo Ducas and Daniele Micciancio	30/5/2017
TFHE	C++/C	-	-	-	+	-	Zama	16/9/2021
Concrete	Rust	-	-	-	+	-	Zama	10/5/2022
HEEAAN	C++	-	-	-	-	+	Seoul National University	27/1/2022
RNS-EAAN	C++	-	-	-	-	+	Kyoohyung and Miran	26/10/2018
FV-NFLlib	C++	-	+	-	-	-	CryptoExperts	26/7/2016
CuFHE	Cuda/C++	-	-	-	+	-	Chillotti	9/2/2019
NUFHE	Python	-	-	-	+	-	NuCypher	18/3/2020
OpenFHE	C++	+	+	+	+	+	Duality Technologies	18/8/2022

III. XULOSA

Ushbu maqolada gomomorfik shifrlash algoritmlari haqida tushunchalar, ularning algoritmlarining algebraik asoslari, shifrlash algoritmlari turlari, qisman gomomrofik shifrlash algoritmlarining tavsifi, chegaralangan gomomorfik shifrlash algoritmlarining xossalari, ideal panjara, butun sonlarga asoslangan, xato bilan o‘rganish, NTRU matematik muammolariga asoslangan to‘liq gomomorfik shifrlash algoritmlari tahlil qilindi hamda gomomorfik shifrlash algoritmlariga oid kriptografik kutubxonalar o‘rganib chiqildi.

Qisman gomomorfik shifrlash algoritmlarining kriptobardoshliligi juda katta sonlardan tashkil topgan kalitlarni generatsiya qilishga bog‘liq. 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 yetarlicha kalit uzunligida tezkor, yuqori kriptobardoshlikka ega gomomorfik shifrlash algoritmlarni shakllantirish kriptologiyaning muhim masalalaridan biri hisoblanadi.

Qo‘shish va ko‘paytirishni qo‘llab-quvvatlaydigan to‘liq gomomorf shifrlash sxemasi ochiq matn maydonining halqa tuzilishini saqlaydi va shuning uchun ancha samaraliroqdir. Bunday sxemadan foydalanish ishonchli bo‘lmagan shaxsga shifrmatnlarning kalitlarini oshkor qilmasdan va maxfiyligini saqlamasdan hisob-kitoblarni amalga oshirishga imkon beradi. Bugungi kunda BGV, BVF, FHEW, TFHECKKS kabi gomomorfik shifrlash algoritmlari to’liq gomomorfik kriptografik tizimlar kutub-xonalarida keng qo’llanilmoqda.

Gomomorfik shifrlar algoritmlarini elektron ovoz berish tizimlari, elektron hukumat, moliya, xavfsizlik tizimlari, sog‘liqni saqlash, bulutli hisoblash tizimlari, narsalar internet tizimlari, suniy intellekt va mashinali o‘qitish kabi bir qancha sohalarda qo‘llash shaxsiy ma’lumotlarni qayta ishlash jarayonida konfidensiallikni ta’minlaydi.

Hozirda IBM, Microsoft, Zama, Duality Technologies kabi bir qancha mashxur kompaniyalar o’zlarining qisman va to’liq gomomorfik shifrlash algoritmlarining kriptografik kutub-xonalarini taklif qilishmoqda. Ushbu kutubxonalar sog’liqni saqlash bazalarida, tasvirlarni qayta ishlash va xavfsiz qidirish tizimlarida ma’lumotlar konfidensialligini ta’minlaydi.

Lekin ushbu sxemani amalga oshirishda samaradorlik, mavjud algoritmlarning murak-kabligi, hisoblash resurslarining cheklanganligi,

hisoblash narxining yuqoriligi kabi bir qancha muammolar mavjud.

Bugungi kunda gomomorfik shifrlash sohasida izlanishlar davom etmoqda va olimlar bu muammolarni hal qilish ustida ish olib bormoqda. Bu usulning imkoniyatlari kelajakda ko‘proq amaliy dasturlarda qo‘llanilishi kutilmoqda.

ADABIYOTLAR

[1] *O‘G‘Li, X. U. U.* (2023). Parametrli algebraga asoslangan El-Gamal shifrlash algoritmlarini gomomorfik xususiyatini tadqiq etish. Al-Farg‘oniy avlodlari, 1(4), 153-157.

[2] *Rass, S., & Slamanig, D.* (2013). Cryptography for security and privacy in cloud computing. Artech House.

[3] *Chatterjee, A., & Aung, K. M. M.* (2019). Fully homomorphic encryption in real world applications. Singapore: Springer.

[4] *Jain, N., & Cherukuri, A. K.* (2023). Revisiting Fully Homomorphic Encryption Schemes. arXiv preprint arXiv:2305.05904

[5] *Asante, G., Hayfron-Acquah, J. B., & Asante, M.* (2021). Evolution of Homomorphic Encryption. International Journal of Computer Applications, 183(29), 37-40.

[6] *Fan, J., & Vercauteren, F.* (2012). Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive.

[7] *Sadi, M.* (2020). Homomorphic encryption. In Emerging Topics in Hardware Security (pp. 281-307). Cham: Springer International Publishing.

[8] *Forouzan, B. A.* (2007). Cryptography & network security. McGraw-Hill, Inc.

[9] *Wainakh, A.* (2018). Homomorphic encryption for data security in cloud computing (Master’s thesis, Middle East Technical University).

[10] *Gentry, C.* (2009, May). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169-178).

[11] *Koç, Ç. K., Özdemir, F., & Özger, Z. Ö.* (2021). Partially Homomorphic Encryption (pp. 37-41). Springer.

[12] *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

[13] *Benzekki, K., El Fergougui, A., & El Alaoui, A. E. B.* (2016). A secure cloud computing architecture using homomorphic encryption. International Journal of Advanced Computer Science and Applications, 7(2).

[14] *Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., Fitzek, F. H., & Aaraj, N.* (2022). Survey on fully homomorphic encryption, theory, and applications. Proceedings of the IEEE, 110(10), 1572-1609.

[15] *Brakerski, Z., & Vaikuntanathan, V.* (2014). Efficient fully homomorphic encryption from (standard) LWE. SIAM Journal on computing, 43(2), 831-871.

[16] *Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V.* (2010). Fully homomorphic encryption over the integers. In Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29 (pp. 24-43). Springer Berlin Heidelberg.

[17] *Brakerski, Z., & Vaikuntanathan, V.* (2011, August). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual cryptology conference (pp. 505-524). Berlin, Heidelberg: Springer Berlin Heidelberg.

[18] *Rivest, R. L., Adleman, L., & Dertouzos, M. L.* (1978). On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), 169-180.

[19] *Goldwasser, S., & Micali, S.* (2019). Probabilistic encryption & how to play mental poker keeping secret all partial information. In Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali (pp. 173-201).

[20] *ElGamal, T.* (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[21] *Benaloh, J. C.* (1986, August). Secret sharing homomorphisms: Keeping shares of a secret secret. In Conference on the theory and application of cryptographic techniques (pp. 251-260). Berlin, Heidelberg: Springer Berlin Heidelberg.

[22] *Paillier, P.* (1999, April). Public-key cryptosystems based on composite degree residuosity classes. In International conference on the theory and applications of cryptographic techniques (pp. 223-238). Berlin, Heidelberg: Springer Berlin Heidelberg.

[23] *Damgård, I., & Jurik, M.* (2001). A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In Public Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001 Cheju Island, Korea, February 13–15, 2001 Proceedings 4 (pp. 119-136). Springer Berlin Heidelberg.

[24] *Boneh, D., Goh, E. J., & Nissim, K.* (2005). Evaluating 2-DNF formulas on ciphertexts. In Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2 (pp. 325-341). Springer Berlin Heidelberg.
[25] *López-Alt, A., Tromer, E., & Vaikuntanathan, V.* (2013). Multikey fully homomorphic encryption and on-the-fly multiparty computation. IACR Cryptology ePrint Archive, 2013.
[26] *Smart, N. P., & Vercauteren, F.* (2010, May). Fully homomorphic encryption with relatively small key and ciphertext sizes. In International Workshop on Public Key Cryptography (pp. 420-443). Berlin, Heidelberg: Springer Berlin Heidelberg.

Поступила в редакцию 20.09.2024

Citation: *Xudoykulov Z.T., Xudoynazarov U.U.* (2024). Gomomorfik shifrlash algoritmlarining umumiy tahlili. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 7(4). – B. 33-47. https://doi.org/10.62132/ijdt.v7i4.217

GENERAL ANALYSIS OF HOMOMORPHIC ENCRYPTION ALGORITHMS

Khudoykulov Z.T.[1], *Khudoynazarov U.U.*[1]
[1] Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
zarif.khudoykulov@tuit.uz, umidjonxudoynazarov@gmail.com

Abstract. *Data privacy issues are increasing significantly in computing systems implemented by the Internet of Things, cloud computing, e-government, artificial intelligence applications, and neural networks. Homomorphic encryption algorithms provide an opportunity to perform algebraic operations on encrypted data without decrypting them. This article explores the algebraic basics needed to understand homomorphic encryption algorithms. The article describes the main fully homomorphic encryption schemes based on various mathematical problems and their fundamental foundations. Cryptographic libraries for homomorphic encryption algorithms and problems related to their implementation are analyzed.*

Keywords: *Homomorphic encryption, fully homomorphic encryption, El-Gamal algorithm, lattices, ideal lattice, factorization, algebraic structures, cloud computing.*

ОБЩИЙ АНАЛИЗ АЛГОРИТМОВ ГОМОМОРФНОГО ШИФРОВАНИЯ

Худойкулов З.Т.[1], *Худойназаров У.У.*[1]
[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хоразми, Ташкент, Узбекистан
zarif.khudoykulov@tuit.uz, umidjonxudoynazarov@gmail.com

Аннотация. *В таких вычислительных системах, как Интернет вещей, системы облачных вычислений, электронное правительство, приложения искусственного интеллекта и нейронные сети, проблемы конфиденциальности данных значительно возрастают. Алгоритмы гомоморфного шифрования дают возможность выполнять алгебраические операции над зашифрованными данными без их расшифровки. В данной статье изучаются алгебраические основы, необходимые для понимания алгоритмов гомоморфного шифрования. В статье описаны основные полностью гомоморфные схемы шифрования, основанные на различных математических задачах, и их фундаментальные основы. Анализируются криптографические библиотеки для алгоритмов гомоморфного шифрования и проблемы, связанные с их реализацией.*

Ключевые слова: *гомоморфное шифрование, полностью гомоморфное шифрование, алгоритм Эль-Гамаля, решетки, идеальная решетка, факторизация, алгебраические структуры, облачные вычисления.*