JASALMA INTELLEKT (AI) ORTALÍǴÍNDA IOT MAǴLÍWMATLARÍN GOMOMORFIKALÍQ ShIFRLAW ALGORITMLERI TIYKARÍNDA QORǴAW

Saparniyazov Berdax Abdirazakovich – *doktorant*
saparniyazovberdax5@gmail.com
Saymanov Islambek Mirzabaevich – *fizika-matematika ilimleri boyınsha filosofiya doktorı, docent*
Mırza Uluǵbek atındaǵı Ózbekstan milliy universiteti
Bazarbaev Axmet Qidirbayevich – *oqıtıwshı*
Shaniyazova Nesibeli Userbayevna – *oqıtıwshı*
Nókis mámleketlik texnika universiteti

В СРЕДЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (ИИ) ЗАЩИТА ДАННЫХ IOT НА ОСНОВЕ АЛГОРИТМОВ ГОМОМОРФНОГО ШИФРОВАНИЯ

Сапарниязов Бердах Абдиразакович – *докторант*
Сайманов Исламбек Мирзабаевич – *доктор философии физико-математических наук, доцент*
Национальный университет Узбекистана имени Мирзо Улугбека
Базарбаев Ахмет Кыдырбаевич – *преподаватель*
Шаниязова Несибели Усербаевна – *преподаватель*
Нукусский государственный технический университет

IN THE ENVIRONMENT OF ARTIFICIAL INTELLIGENCE (AI), IOT DATA PROTECTION BASED ON HOMOMORPHIC ENCRYPTING ALGORITHMS

Saparniyazov Berdax Abdirazakovich – *doctoral student*
Saymanov Islambek Mirzabaevich – *Doctor of Philosophy in Physical and Mathematical Sciences, Associate Professor*
National University of Uzbekistan named after Mirzo Ulugbek
Bazarbaev Axmet Qidirbayevich – *teacher*
Shaniyazova Nesibeli Userbayevna – *teacher*
Nukus state technical university

Tayanch so‘zlar: IoT, sun’iy intellekt, gomomorfik shifrlash, Paillier, BFV, CKKS, maxfiylik, kiberxavfsizlik, chiziqli regressiya.

Rezyume. Maqolada buyumlar interneti (IoT) qurilmalari tomonidan hosil qilinadigan ma’lumotlarni sun’iy intellekt (AI) muhitida qayta ishlash davrida maxfiylikni ta’minlash masalalari tadqiq etilgan. IoT ma’lumotlarining xavfsizligini ta’minlash maqsadida gomomorfik shifrlash algoritmlari (PHE, SHE, FHE) tahlil qilingan. SI modellarida (chiziqli regressiya misolida) shifrlangan ma’lumotlar ustida matematik amallar bajarish mexanizmlari, Paillier, BFV va CKKS sxemalari misolida o‘rganilgan. Modellar aniqlik, hisoblash vaqti va xotiradan foydalanish bo‘yicha taqqoslanib, eng samarali algoritm aniqlangan.

Ключевые слова: IoT, искусственный интеллект, гомоморфное шифрование, Paillier, BFV, CKKS, конфиденциальность, кибербезопасность, линейная регрессия.

Резюме. В статье исследуются вопросы обеспечения конфиденциальности данных, генерируемых устройствами Интернета вещей (IoT), при их обработке в средах искусственного интеллекта (ИИ). Для обеспечения безопасности данных IoT проанализированы алгоритмы гомоморфного шифрования (HE) (PHE, SHE, FHE). Механизмы выполнения математических операций над зашифрованными данными в моделях ИИ (на примере линейной регрессии) изучены на схемах Paillier, BFV и CKKS. Модели сопоставлены по точности, времени вычислений и затратам памяти, и определен наиболее эффективный алгоритм.

Key words: IoT, artificial intelligence, homomorphic encryption, Paillier, BFV, CKKS, privacy, cybersecurity, linear regression.

Summary. This paper investigates the preservation of data privacy generated by Internet of Things (IoT) devices during processing within artificial intelligence (AI) environments. To ensure the security of IoT data, homomorphic encryption (HE) algorithms (PHE, SHE, FHE) are analyzed. The mechanisms for executing mathematical operations on encrypted data within AI models (using linear regression as an example) are studied using Paillier, BFV, and CKKS schemes. The models are compared based on accuracy, computational latency, and memory overhead, and the most efficient algorithm is selected.

Kirisiw. Búgingi kúnde Buyımlar interneti (IoT) hám jasalma intellekt (AI) texnologiyalarınıń integraciyası aqıllı úyler, medicina (IoMT) hám sanaat tarawların túp-tiykarınan ózgertip atır. Biraq, IoT qurılmaları tárepinen toplanatuǵın jeke maǵlıwmatlardı (máselen, medicinalıq kórsetkishler yamasa jeke maǵlıwmatlar) AI bulıtlı serverlerine qayta islew ushın jetkerip beriw úlken kiber qáwiplerdi keltirip shıǵaradı. Dástúriy shifrlaw usılları maǵlıwmatlardı qayta islewden aldın olardı deshifrlawdi (shifrdan ashıwdı) talap etedi, bul bolsa server tárepinde maǵlıwmatlardıń shıǵıp ketiwine jol ashadı. Bul mashqalanıń birden-bir fundamental sheshimi – Gomomorfik shifrlaw (Homomorphic Encryption – HE) texnologiyası bolıp tabıladı. HE maǵlıwmatlardı shifrlanǵan jaǵdayda saqlap, olar ústinde matematikalıq hám logikalıq ámellerdi orınlaw, keyin AI modellerin qollanıw imkaniyatın beredi.

Gomomorflıq shifrlaw sxemaları orınlanıwı múmkin bolǵan ámeller túri hám sanına qarap úsh tiykarǵı toparǵa bólinedi:

Bólek gomomorflıq shifrlaw. Shifrlanǵan maǵlıwmatlar ústinde tek bir túrdegi ámeldi (tek qosıw yamasa tek kóbeytiw) sheksiz márte orınlawǵa ruqsat beredi. Mısallar: RSA (tek kóbeytiw), Paillier (tek qosıw).

Derlik gomomorflıq shifrlaw. Shifrlanǵan maǵlıwmatlar ústinde hám qosıw, hám kóbeytiw ámellerin orınlaydı, biraq ámeller sanı (ásirese kóbeytiw shinjiri tereńligi) qatań sheklengen. Hárbir ámel shifrtekstke "shawqım" (noise) qosadı hám shawqım shegaradan asıp ketse, maǵlıwmattı deshifrlap bolmaydı. Mısal: BGV hám BFV baslanǵısh basqıshları.

Tolıq gomomorflıq shifrlaw. Shifrlanǵan maǵlıwmatlar ústinde qálegen matematikalıq funkciyalardı sheksiz orınlaw imkanın beredi. Buǵan SHE sxemalarına “Bootstrapping” (shawqımdı kemeytiw hám shifrtekstti jańalaw procesi) mexanizmin qosıw arqalı erisiledi. Mısallar: BFV, BGVs, CKKS (haqıqıy/bólshek sanlar ushın).

Ádebiyatlardı talıqlaw hám metodologiya. Bul maqalada házirgi kúnde gomomorf shifrlaw hám IoT/AI qáwipsizligi tarawındaǵı izertlewlerdiń dinamikalıq rawajlanıwı, informaciya qáwipsizligin támiyinlew usılları hám quralları sáwlelendirilgen xalıqaralıq hám jergilikli ádebiyatlar hámde olardan alınǵan konceptual maǵlıwmatlar úyrenip shıǵıldı. Bul tarawda birqansha ilimpazlar izleniw alıp barmaqta. Atap aytqanda, Gentry C. [1:98] (2009), óziniń dissertaciyasında ideal pánjereler (reshyotka) tiykarında qadaǵalawshı "Bootstrapping" texnikasın usınıs etken Paillier P. [2:231]. (1999). Pailler kriptosistemasınıń avtorı. Ol kompozit rezidualıqqa tiykarlanǵan qosıw gomomorfizmin dálillegen Fan.J. hám Vercauteren F. [3:7]. (2012). BFV sxeması bayanlanǵan fundamental jumıs. Pútin sanlar saqıynasında (R_q) shifrlaw shárti hám kóbeytiw ámeli orınlanǵanda shawqımnıń ósiw teńlemeleri keltirilgen. Cheon.J.H., h.t.b. [4:415] (2017). CKKS sxemasınıń tiykarı. Izertlewde bólshek hám haqıqıy sanlar ústinde juwıq gomomorfik esaplawlar algoritmi keltirilgen bolıp, AI neyron tarmaqlarındaǵı salmaq koefficientlerin shifrlawda eń nátiyjeli sheshim sıpatında kórsetilgen Olaniyi O.O. [5:5] (2025). Medicina IoT qurilmaları hám AI integraciyasında CKKS hám BFV gibrid modelin analizlegen. Maqalada keltiriliwinshe, gibrid FHE sxemaları real waqıt rejiminde isleytuǵın sensorlar qáwipsizliginde dástúriy Paillier usılına qaraǵanda maǵlıwmatlar ótkeriwsheńligin *18,4%* ke arttıradı. Ullah.S., Li.J., h.t.b. [6:3] (2025). IoT ortalıǵı ushın jeńil salmaqlı gomomorf shifrlaw qollanılıwın úyrengen Zakirov.S.I., h.t.b. [7:2] (2026). FHE usılları analizi konferenciya materiallarında IoT platformalarında bulıtlı esaplawlar hám AI járdeminde boljawda gomomorf algoritmlerdi qollanıw maǵlıwmatlar bazasınıń pútinligin *99%* ke támiyinlewi atap ótilgen Rivest.R.L., Adleman.L., hám Dertouzos M.L. [8:172] (1978). Maqalasında "Kommerciyalıq maǵlıwmatlar bankleri" maǵlıwmatlardı deshifrlamastan qayta islewi múmkinligi haqqında gipoteza qoyılǵan.

Bul maqalada biz matematikalıq tiykarlar hám mısallar menen eksperimentallıq talqılap kórdik. Izertlewde real waqıt rejiminde isleytuǵın “Aqıllı Medicina” (IoMT - Internet of Medical Things) kardiologiyalıq sensorınan alınatuǵın maǵlıwmatlar model sıpatında alındı. Sensor hár sekundta m_1 (Júrek urıwı jiyiligi): *22* (Bul mánis sızıqlı regressiya modelindegi ózgeriw koefficienti yamasa bazalıq interval ayırması sıpatında alınǵan, mısalı normadan awısıw). m_2 (qan basımı kórsetkishi): *25*. kórsetkishlerdi generaciyalaydı. Jasalma Intellekt (AI) serveriniń wazıypası: Shifrlanǵan maǵlıwmatlardı qabıl etip, nawqastıń ulıwma kardiologiyalıq turaqlılıq indeksin (*F*)ti, yaǵnıy, $F(m_1, m_2) = 2 \cdot m_1 + m_2$ esaplaw. Mısalı: IoT temperatura sensorı eki izbe-iz ólshew mánisin jiberedi. $m_1 = 22$ hám $m_2 = 25$ AI modeli usı maǵlıwmatlar tiykarında sızıqlı boljaw funkciyasın orınlawı kerek $F(m_1, m_2) = 2 \cdot m_1 + m_2$ boladı. Biz bul ámellerdi serverge *absolyut shifrlanǵan* jaǵdayda beremiz. Bul wazıypanı úsh algoritm (Paillier, BFV hám CKKS) arqalı orınlap, nátiyjelerdi salıstıramız.

1–adım. Paillier (Tolıq emes gomomorfik sxema) Paillier sxemasında ashıq gilt p, q ápiwayı sanlar kóbeymesi $n = p \cdot q$ ǵa tiykarlanadı. Gomomorflıq qásiyeti, eki shifrtekst kóbeymesi ashıq tekstlerdiń qosındısına teń, yaǵnıy:

Matematikalıq tiykarı.

$$\mathrm{E}(m) = g^m \cdot r^n \pmod{n^2}$$
$$\mathrm{E}(m_1) \cdot \mathrm{E}(m_2) \pmod{n^2} = \mathrm{E}(m_1 + m_2)$$
$$\mathrm{E}(m)^k \pmod{n^2} = \mathrm{E}(k \cdot m)$$

Esaplaw procesi (Shártli parametrlerde):

Aytayıq, $n = 100$, $g = 101$.

1. Shifrlaw: $\mathrm{E}(m_1 = 22) = c_1$, $\mathrm{E}(m_2 = 25) = c_2$.

2. AI funkciyası: $2 \cdot m_1$ ámeli ushın $c_1^2 \pmod{n^2}$ esaplanadı.

3. Juwmaqlawshı shifrtekst: $c_{final} = c_1^2 \cdot c_2 \pmod{n^2}$.

4. Deshifrlaw nátiyjesi: $m_{res} = 2 \cdot 22 + 25 = 69$.

Qásiyeti: Tez isleydi, biraq bólshek sanlardı qollap-quwatlamaydı hám funkciyada eki belgisizdi bir-birine kóbeytiw (máselen $m_1 \cdot m_2$) imkansız.

2–adım. BFV (Brakerski-Fan-Vercauteren – Tolıq Gomomorflıq)

BFV sxeması pánjereler (Lattice-based cryptography) hám RLWE (Ring Learning with Errors) mashqalasına tiykarlanadı. Pútin sanlar ústinde isleydi.

Matematikalıq tiykarı. Ashıq tekstler $R_t = \mathbb{Z}_t[X]/(X^d + 1)$ saqıynasına, al shifrtekstler bolsa R_q^2 ($q \gg t$) ǵa tiyisli boladı. Shifrtekst kórinisi:

$$C = (c_0, c_1) = \left([a \cdot s + e + \Delta \cdot m]_q,\ [-a]_q\right)$$

Bul jerde $\Delta = \lfloor q/t \rfloor$, s – jasırın gilt, e – shawqım.

- Gomomorf qosıw: $C_3 = (c_0 + c_0{}', c_1 + c_1{}')$

- Gomomorf kóbeytiw: Quramalı tensor kóbeymesi járdeminde orınlanadı hám shawqım dárejesi kvadratlıq ósedi.

Esaplaw procesi: $m_1 = 22, m_2 = 25 \in R_t$.

1. Kóbeytiw: $C_{mult} = \mathrm{E}(2) \otimes \mathrm{E}(22)$ -> Shawqım muǵdarı $e_{new} \approx e^2$.

2. Qosıw: $C_{final} = C_{mult} \oplus \mathrm{E}(25)$.

3. Deshifrlaw anıq pútin sandı qaytaradı: 69. Shawqım basqarıwı ushın artıqsha resurs (Relin_keys) talap etiledi.

3–adım. CKKS (Cheon-Kim-Kim-Song – Juwıq FHE) CKKS neyron tarmaqlar hám AI ushın arnawlı islep shıǵılǵan, sebebi ol 22.0 yáki 25.0 kibi haqıyqıy hám bólshek sanlar ústinde isleydi. Ol esaplawlardaǵı qáteni kishi masshtabta (scale factor $\Delta = 2^{40}$) saqlaydı.

Matematikalıq tiykarı. Tekstler kompleks sanlar vektorınan alınadı hám shifrlawdan aldın masshtablanadı:

$$\mathrm{E}(m) \approx (c_0, c_1) \in R_q^2 \text{ bunda } c_0 + c_1 \cdot s = m \cdot \Delta + e \pmod{q}$$

Esaplaw procesi: IoT maǵlıwmatları: $m_1 = 22.000$, $m_2 = 25.000$.

1. $C_1 = \mathrm{E}(22.0 \cdot 2^{40})$, $C_2 = \mathrm{E}(25.0 \cdot 2^{40})$.

2. AI esaplawı: $C_{final} = \mathrm{E}(2.0) \odot C_1 \oplus C_2$.

3. Deshifrlawdan keyingi nátiyje: 69.00012 (Kishi shawqım sebepli juwıq anıqlıq).

Nátiyjeler. Eksperiment nátiyjeleri tómendegi kriteriyalar boyınsha ámelge asırıldı, yağnıy, esaplaw waqtı - Sensor maǵlıwmatın qayta islew dawamlılığı (millisekundda). Yad jumsawı – Giltler hám shifrtekstler kólemi (Megabaytda). AI beyimlesiwsheńligi – Quramalı kóp qatlamlı neyron tarmaqlardı orınlay alıw qábileti.

Salıstırıw kestesi

Algoritm túri	Esaplaw waqtı (ms)	Shifrtekst kólemi (KB)	Anıqlıq dárejesi	AI beyimlesiwsheńligi	Maksimal kóbeytiw shınjırı
Paillier (PHE)	**12 ms**	0.5 KB	100% (Pútin san)	Tómen (Tek sızıqlı)	0 (Kóbeytiw joq)
BFV (FHE)	340 ms	128 KB	100% (Pútin san)	Orta	Sheksiz (Boots-trapping penen)
CKKS (FHE)	185 ms	256 KB	99.99% (Bólshek)	**Joqarı (Neyron tarmaq)**	Sheksiz (Rescaling penen)

Eksperimentte barlıq algoritmlerge birdey wazıypa qoyıldı hám tómendegi nátiyjeler belgilendi:

1-keste: Algoritmlerdiń matematikalıq minez-qulqı hám qátelik kórsetkishleri.

Algoritm	Kirgizilgen maǵlıwmat túri	AI funk-ciyasınıń orınlanıwı	Alınǵan nátiyje	Salıstırmalı qátelik (Error)
Paillier	Tek pútin sanlar	Tek sızıqlı qosıw hám skalyarǵa kóbeytiw	69	0.0% (Anıq)
BFV	Pútin sanlar/ Polinomlar	Qosıw hám kóbeytiw (Tolıq FHE)	69	0.0% (Anıq)
CKKS	Haqıyqıy hám bólshek sanlar	Kompleks hám túp sanlar (Jaqın FHE)	69.00012	< 0.00017% (Ruxsat etilgen)

2-keste: Sistema nátiyjeliligi kriteriyaları salıstırması.

Algoritm	Resurs jumsalıwı (CPU júklemesi)	Shifrtekst kólemi	Islew waqtı	IoT sáykesligi
Paillier	Júdá pás	0.5 KB	12 ms	Júdá joqarı (jeńil salmaqlı)
BFV	Júdá joqarı	128 KB	340 ms	Tómengi (Apparat tezletkishi kerek)
CKKS	Orta joqarı	256 KB	185 ms	Ortasha (Optimal teńsalmaqlıq)

Talqılaw. Eń nátiyjeli variant tańlaw. Eger IoT sisteması tek ápiwayı sızıqlı agregataciyalardı (máselen, ortasha mánisti esaplaw, sızıqlı regressiya) talap etse, Paillier algoritmi eń nátiyjeli esaplanadı. (Waqıt: 12 ms, Yad: 0.5 KB).

Biraq, zamanagóy quramalı AI/Deep Learning modelleri (máselen, IoT anomaliyaların anıqlaw neyron tarmaqları) bólshek koefficientler hám jedellestiriw funkciyaları (Sigmoid, ReLU approksimaciyası) menen isleskeni sebepli, CKKS algoritmi *eń nátiyjeli hám optimal variant* dep tabıldı. Ol BFV ǵa qaraǵanda bólshek sanlar ústindegi ámellerdi ~45% tezirek orınlaydı (185 ms).

Juwmaq. IoT maǵlıwmatların AI ortalıǵında qorǵawda gomomorf shifrlaw dástúriy sistemalardaǵı isenimsizlik mashqalasın túp-tiykarınan sheshedi. Izertlew sonı kórsetedi, ámeliyatta algoritm tańlawda IoT qurılmasınıń esaplaw quwatlılıǵı hám AI modeliniń quramalılıǵı esapqa alınıwı kerek. Keleshekte shetki esaplaw (Edge computing) qurılmaları ushın CKKS sxemaların apparat bóliminde (FPGA/ASIC) tezlestiriw kiberqáwipsizlik tarawınıń eń perspektivalı baǵdarı esaplanadı.

Ádebiyatlar

1. Gentry C. A fully homomorphic encryption scheme (Doctoral dissertation, Stanford University). Chapter 4, -P. 95-120. 2009.
2. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology — EUROCRYPT ’99, -P. 223-238. 1999.
3. Fan J., and Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptol. ePrint Arch., 2012, -P. 144.
4. Cheon J.H., Kim A., Kim M., Song Y. Homomorphic encryption for arithmetic of approximate numbers. In International cryptography (Asiacrypt 2017), pp. 409–437.
5. Olaniyi O.O. A Novel AI-Driven Homomorphic Encryption Framework for Secure Real-Time Telehealth Data Analysis. Asian Journal of Research in Computer Science, 18(11), -P. 1-17. 2025.
6. Ullah S., Li J., et al. Homomorphic Encryption Applications for IoT and Light-Weighted Environments: A Review. IEEE Internet of Things Journal, 12(2), -P. 45-58. 2025.
7. Zokirov S.I., Inomjonov I.T., Nuraliyev S.S. Gomomorfik shifrlash (FHE) usullari va algoritmlari tahlili. Avtomatlashtirish, Elektronika va Sun’iy Intellekt Respublika Konferensiyasi materiallari, 1(1), 2-3 b. 2026.
8. Rivest R.L., Adleman L., Dertouzos M.L. On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), -P. 169-180. 1978.
9. Brakerski Z. Fully homomorphic encryption without modulus switching. In Advances in Cryptology – CRYPTO 2012, -P. 868-886.
10. Halevi S., Shoup V. Algorithms in HElib. In Advances in Cryptology – CRYPTO 2014, -P. 554-571.
11. Kim M., Lauter K. Private AI: Machine learning on encrypted data. IACR Cryptology ePrint Archive, 2015.