KRITIK INFRATUZILMALARDA MAXFIYLIKNI SAQLAYDIGAN SUN'IY INTELLEKT UCHUN KVANT-HIMOYALANGAN FEDERATIV TA'LIM ARXITEKTURASI

Гаипназаров Р.Т.[1], **Азимова У.А.**[2], **Жумакулов Б.С.**[3]

[1,2]*O‘qituvchi, “Raqamli texnologiyalar konvergentsiyasi” kafedrasi, Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston.*
[3]*O‘qituvchi, “Sun’iy intellekt” kafedrasi, Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston.*
[1]*e-mail: gaipnazarovs.uds@gmail.com,* [2]*e-mail: umidaazimova64@gmail.com,*
[3]*e-mail: baxajann0@gmail.com*

Annotatsiya: Ma’lumotlarga asoslangan sun’iy intellekt (AI) modellari va foydalanuvchi maxfiyligi o‘rtasidagi ziddiyat bugungi kunning asosiy muammolaridan biridir. Federativ ta’lim (FL) markazlashtirilmagan holda modellarni o‘qitish orqali bu muammoni hal qilishga qaratilgan istiqbolli yondashuv hisoblanadi. Biroq, FL tizimlarida model yangilanishlarini himoya qilish uchun qo‘llaniladigan klassik kriptografik protokollar yaqinlashib kelayotgan kvant hisoblashlari tahdidi oldida zaifdir. Ushbu tadqiqotda biz **Q-Fed (Quantum-Resistant Federated Learning)** deb nomlangan yangi arxitekturani taklif etamiz. Q-Fed federativ ta’lim jarayonini post-kvant kriptografiyasi (PQC) algoritmlari bilan integratsiya qilib, tizimni ham klassik, ham kvant hujumlaridan himoya qiladi. Biz panjaraga asoslangan CRYSTALS-Kyber (KEM) va CRYSTALS-Dilithium (imzo) sxemalarini qo‘llagan holda arxitekturani ishlab chiqdik va uning samaradorligini keng qamrovli simulyatsiyalar orqali tahlil qildik. Natijalar shuni ko‘rsatadiki, Q-Fed model aniqligini pasaytirmagan holda kvant-barqaror xavfsizlikni ta’minlaydi, biroq hisoblash va kommunikatsiya xarajatlarida o‘lchanadigan, ammo boshqariladigan ortish kuzatiladi. Ushbu ish kelajak avlod AI tizimlarining maxfiyligi va xavfsizligini ta’minlash uchun amaliy va istiqbolli yechim taklif etadi.

Kalit so‘zlar: Federativ ta'lim, post-kvant kriptografiyasi, mashinaviy ta'lim, kiberxavfsizlik, maxfiylikni saqlash, kvant hisoblashlari.

KIRISH (INTRODUCTION)

Raqamli transformatsiya davri bizga misli ko‘rilmagan imkoniyatlar bilan birga, hal qilinishi kerak bo‘lgan murakkab muammolarni ham taqdim etdi. Sun'iy intellekt (AI) va mashinaviy ta'lim (ML) sog'liqni saqlashdan tortib moliyaviy xizmatlargacha bo‘lgan deyarli barcha sohalarni inqilob qilmoqda. Biroq, bu aqlli tizimlarning "yoqilg'isi" – ma'lumotlardir. Qanchalik ko‘p va sifatli ma'lumot bo‘lsa, model shunchalik aniq va foydali bo‘ladi. Bu esa fundamental ziddiyatni keltirib chiqaradi: bir tomondan innovatsiyalar uchun ma'lumotlar kerak, ikkinchi tomondan esa foydalanuvchilarning shaxsiy ma'lumotlari daxlsizligi va maxfiyligini ta'minlash shart [1].

Bu muammoning an'anaviy yechimi ma'lumotlarni markaziy serverga to‘plash edi, biroq bu yondashuv ma'lumotlarning sizib chiqishi, suiiste'mol qilinishi va yagona nuqtadagi zaiflik (single point of failure) kabi jiddiy xavflarni yuzaga keltiradi. Aynan shu nuqtada, federativ ta'lim (FL) sahnaga chiqadi [2]. FL go‘yo turli shifoxonalardagi bir guruh shifokorlarga o‘xshaydi: ular o‘z bemorlarining maxfiy tibbiy kartalarini bir-biriga ko‘rsatmasdan, o‘z tajribalari va bilimlari (ya'ni, model og'irliklari) bilan o‘rtoqlashib, birgalikda aniqroq tashxis qo‘yishni o‘rganishadi. Ya'ni, ma'lumotlar o‘z egasining qurilmasida (telefon, kompyuter) qoladi va faqat modelning o‘zi markaziy serverga yuboriladi.

Ammo bu go‘zal me'morchilikning ham o‘z "Axilles tovoni" bor. Model yangilanishlari tarmoq orqali uzatilayotganda, ularni ruxsatsiz kirishdan himoya qilish uchun klassik kriptografik protokollar (masalan, TLS) qo‘llaniladi. Bu protokollar bugungi kunda ishonchli bo‘lsa-da, ularning poydevori – katta sonlarni ko‘paytuvchilarga ajratishning murakkabligi kabi matematik muammolar – ufqda

ko‘rinayotgan bo‘ron, ya'ni kvant kompyuterlari oldida dosh berolmaydi. Shor algoritmi [3] kabi kvant algoritmlari bugungi shifrlash standartlarini osongina buzish qudratiga ega bo‘ladi. Bu esa federativ tarmoqlardagi barcha ma'lumotlar almashinuvini xavf ostiga qo‘yadi.

Ushbu "kvant tahdidi" ga javoban, kriptografiya hamjamiyati post-kvant kriptografiyasi (PQC) deb nomlanuvchi yangi avlod algoritmlarini ishlab chiqmoqda [4]. Bu algoritmlar kvant kompyuterlari uchun ham murakkab bo‘lgan matematik muammolarga asoslangan.

Ushbu tadqiqotning asosiy hissasi – ana shu ikki kuchli g'oyani birlashtirishdir. Biz FL ning maxfiylikni saqlovchi tabiatini PQC ning kelajakka yo‘naltirilgan xavfsizligi bilan uyg'unlashtirgan **Q-Fed (Quantum-Resistant Federated Learning)** nomli yangi arxitekturani taklif qilamiz va tahlil qilamiz. Bizning maqsadimiz quyidagilardan iborat:

1. FL jarayoniga PQC algoritmlarini samarali integratsiya qilish sxemasini ishlab chiqish.
2. Taklif etilgan arxitekturaning model aniqligi, hisoblash va kommunikatsiya samaradorligiga ta'sirini baholash.
3. Kvant-barqaror xavfsizlik va tizim unumdorligi o‘rtasidagi muvozanatni (trade-off) o‘rganish.

Ushbu tadqiqot natijalari O‘zbekistonning rivojlanayotgan raqamli iqtisodiyoti, xususan, bank, telekommunikatsiya va sog‘liqni saqlash kabi kritik infratuzilmalarida AI ni xavfsiz joriy etish uchun amaliy qo‘llanma bo‘lib xizmat qilishi mumkin.

Maqolaning keyingi qismlari quyidagicha tuzilgan: II bo‘limda mavzuga oid oldingi ishlar tahlil qilinadi. III bo‘limda taklif etilayotgan Q-Fed arxitekturasi batafsil bayon etiladi. IV bo‘limda eksperimental natijalar keltiriladi, V bo‘limda esa ushbu natijalar muhokama qilinadi. Nihoyat, VI bo‘limda xulosalar va kelajakdagi tadqiqot yo‘nalishlari ko‘rsatiladi.

ADABIYOTLAR SHARHI (RELATED WORKS)

Tadqiqotimiz uchta asosiy yo‘nalish kesishmasida joylashgan: federativ ta'lim, uning xavfsizlik muammolari va post-kvant kriptografiyasi.

Federativ ta'lim. Google tomonidan taklif etilgan FedAvg algoritmi [2] federativ ta'lim sohasida fundamental ish hisoblanadi. U iterativ jarayon bo‘lib, har bir raundda mijozlar (clients) o‘zlarining mahalliy ma'lumotlarida global modelni o‘qitadi, so‘ngra yangilangan og'irliklarni serverga yuboradi. Server esa bu yangilanishlarni o‘rtachalashtirib, yangi global modelni hosil qiladi. Shundan so‘ng, ko‘plab variantlar taklif etildi, masalan, FedProx [5] statistik heterogenlik muammosini hal qilishga qaratilgan bo‘lsa, boshqalari kommunikatsiya samaradorligini oshirishga e'tibor qaratdi.

Federativ ta'limda xavfsizlik. FL ma'lumotlarni lokal saqlasa-da, u turli hujumlardan holi emas. Bularga "zaharlash" hujumlari (poisoning attacks) [6], ya'ni ishtirokchilarning ataylab noto‘g'ri ma'lumot yuborishi orqali global modelga zarar yetkazishi, hamda "xulosa chiqarish" hujumlari (inference attacks) [7], ya'ni uzatilgan model yangilanishlaridan asl ma'lumotlarni qayta tiklashga urinishlar kiradi. Bu hujumlarning oldini olish uchun differensial maxfiylik (differential privacy) va homomorf shifrlash (homomorphic encryption) kabi usullar taklif etilgan. Biroq, bu usullar ham klassik kriptografiyaga tayanadi va kvant tahdidi oldida zaif bo‘lishi mumkin.

Post-kvant kriptografiyasi (PQC). AQSH Milliy Standartlar va Texnologiyalar Instituti (NIST) PQC standartlashtirish jarayonini boshlab, bir necha yillik sinovlardan so‘ng, panjaraga asoslangan (lattice-based), kodga asoslangan (code-based), xeshga asoslangan (hash-based) va boshqa turdagi algoritmlarni standart sifatida tavsiya etdi [4, 8]. Bizning tadqiqotimiz uchun panjaraga asoslangan CRYSTALS-Kyber (kalit almashinuvi uchun) va CRYSTALS-Dilithium (raqamli imzo uchun) sxemalari alohida qiziqish uyg'otadi, chunki ular samaradorlik va xavfsizlikning yaxshi muvozanatini ta'minlaydi.

Tadqiqotdagi bo‘shliq. FL va PQC ni birlashtirish g'oyasi yangi bo‘lsa-da, bu sohadagi ishlar hali dastlabki bosqichda. Ba'zi tadqiqotlar [9] nazariy jihatdan bu imkoniyatni ko‘rib chiqqan, ammo amaliy simulyatsiyalar va unumdorlikning chuqur tahlilini taqdim etmagan. Bizning ishimiz ana shu bo‘shliqni to‘ldirishga, ya'ni PQC ni FL ga integratsiya qilishning amaliy arxitekturasini taklif etishga va uning real sharoitlarga yaqin simulyatsiyalarda har tomonlama tahlilini o‘tkazishga qaratilgan.

METODOLOGIYA (METHODS)

Ushbu bo‘limda biz taklif qilayotgan Q-Fed arxitekturasini batafsil ko‘rib chiqamiz. Avval standart FL jarayonini, so‘ngra xavf modelini va nihoyat, PQC integratsiyasi bilan kuchaytirilgan yangi arxitekturani tavsiflaymiz.

Dastlabki tushunchalar: FedAvg algoritmi: Standart FedAvg [2] quyidagi bosqichlardan iborat:

1. **Initsializatsiya:** Server global modelni (w_0) yaratadi va uni barcha ishtirokchi mijozlarga ($C_1, C_2, ..., C_k$) yuboradi.

2. **Mahalliy o‘qitish:** Har bir raund (t) da, mijozlarning bir qismi tanlab olinadi. Har bir tanlangan mijoz (C_i) global modelni (w_t) o‘zining mahalliy ma'lumotlar to‘plami (Di) asosida bir necha epoxa davomida o‘qitadi va yangi mahalliy model $\left(w_{t+1}^{i}\right)$ hosil qiladi.

3. **Yangilanishlarni yuborish:** Har bir mijoz hisoblangan yangilanishni $\left(\Delta w_i = w_{t+1}^{i} - w_t\right)$ serverga yuboradi.

4. Agregatsiya: Server barcha mijozlardan kelgan yangilanishlarni ularning ma'lumotlar to‘plami hajmiga mutanosib ravishda o‘rtachalashtiradi va yangi global modelni yaratadi:

$$w_{t+1} = w_t + \sum_{i=1}^{k} \frac{n_i}{n} \Delta w_i$$

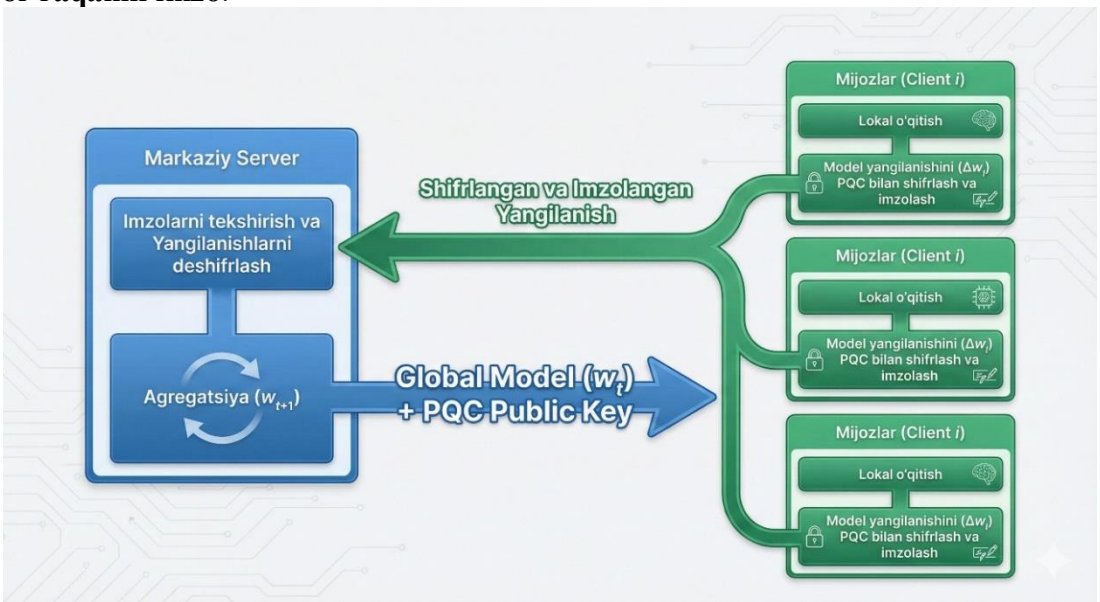
Bu yerda n_i – i\-mijozning ma'lumotlar hajmi, n esa umumiy ma'lumotlar hajmi.

5. **Takrorlash:** Jarayon model kerakli aniqlikka erishguncha 2-4 bosqichlarni takrorlaydi.

Xavf modeli (Threat Model): Biz quyidagi xavf modelini ko‘rib chiqamiz:

- **Server:** "Halol, ammo qiziquvchan" (Honest-but-curious). Server protokolga to‘liq rioya qiladi, lekin mijozlardan kelayotgan yangilanishlarni tahlil qilib, ular orqali ishtirokchilarning shaxsiy ma'lumotlari haqida xulosa chiqarishga urinishi mumkin.
- **Tashqi kuzatuvchi:** Tarmoq trafigini kuzata oladigan kuchli raqib. Bu raqib kelajakda kvant kompyuteriga ega bo‘lishi mumkin ("Store now, decrypt later" hujumi). Uning maqsadi – uzatilayotgan model yangilanishlarini ushlab qolib, keyinchalik kvant kompyuteri yordamida shifrini yechish.

Taklif etilayotgan Q-Fed arxitekturasi: Q-Fed arxitekturasi FedAvg asosiga qurilgan, lekin mijoz va server o‘rtasidagi har bir aloqa seansini post-kvant kriptografiyasi yordamida himoya qiladi. Jarayon quyidagi ikki asosiy komponentdan iborat: **kvant-barqaror kalit almashinuvi** va **kvant-barqaror raqamli imzo**.



Rasm 1. Q-Fed arxitekturasining sxematik diagrammasi

1. Kvant-barqaror kalit almashinuvi (Quantum-Safe Key Exchange):

Har bir model yangilanishini shifrlash uchun simmetrik kalit kerak. Bu kalitni xavfsiz almashish uchun biz NIST tomonidan standartlashtirilgan **CRYSTALS-Kyber** [10], ya'ni Kalit Inkapsulyatsiyasi Mexanizmidan (KEM) foydalanamiz.

- Server o‘zining Kyber ochiq/yopiq kalitlar juftligini (pk_S, sk_S) yaratadi.
- Har bir aloqa seansidan oldin, mijoz (C_i) serverning ochiq kalitidan (pk_S) foydalanib, simmetrik kalit (ss_i) va uning shifrlangan ko‘rinishini (c_i) hosil qiladi (encapsulation).
- Mijoz c_i ni serverga yuboradi. Server o‘zining yopiq kaliti (sk_S) yordamida c_i dan simmetrik kalitni (ss_i) tiklaydi (decapsulation).

Endi mijoz va server faqat ikkisiga ma'lum bo‘lgan ss_i kalitiga ega.

2. Kvant-barqaror raqamli imzo (Quantum-Safe Digital Signature):

Yangilanishlar nafaqat maxfiy, balki autentik bo‘lishi kerak, ya'ni server ularni haqiqatan ham legitim mijozdan kelganiga ishonch hosil qilishi lozim. Buning uchun biz **CRYSTALS-Dilithium** [11] raqamli imzo algoritmidan foydalanamiz.

- Har bir mijoz o‘zining Dilithium ochiq/yopiq kalitlar juftligini (pk_i, sk_i) yaratadi va ochiq kalitni serverda ro‘yxatdan o‘tkazadi.
- Mijoz shifrlangan model yangilanishini yuborishdan oldin, uni o‘zining yopiq kaliti (sk_i) bilan imzolaydi.
- Server yangilanishni qabul qilgach, mijozning ochiq kaliti (pk_i) yordamida imzoni tekshiradi.

Quyida Q-Fed ning bir raundi uchun psevdokod keltirilgan:

```
Algorithm 1: Q-Fed Training Round

1: Server:
2: Initialize global model w_0
3: Generate PQC key pair (pk_S, sk_S) for KEM
4: Broadcast w_0 and pk_S to all clients

5: for each round t = 1, 2, ... do
6: Select a subset of clients C_t
7: for each client C_i in C_t in parallel do
8: // Client-side execution
9: w_t+1_i ← LocalUpdate(w_t, D_i)
10: Δw_i ← w_t+1_i - w_t
11: // Generate session key and encrypt it
12: (ss_i, c_i) ← Kyber.Encaps(pk_S)
13: // Encrypt the model update with the session key
14: encrypted_Δw_i ← AES.Encrypt(ss_i, Δw_i)
15: // Sign the encrypted update
16: signature_i ← Dilithium.Sign(sk_i, encrypted_Δw_i)
17: Send (c_i, encrypted_Δw_i, signature_i) to Server
18: end for

19: // Server-side execution
20: Initialize empty update list U
21: for each received (c_i, encrypted_Δw_i, signature_i) do
22: // Verify signature
23: if Dilithium.Verify(pk_i, encrypted_Δw_i, signature_i) then
24: // Decrypt session key
25: ss_i ← Kyber.Decaps(sk_S, c_i)
26: // Decrypt the model update
27: Δw_i ← AES.Decrypt(ss_i, encrypted_Δw_i)
28: Add Δw_i to U
29: end if
```

```
30: end for
31: // Aggregate updates
32: w_t+1 ← w_t + Aggregate(U)
33: Broadcast w_t+1 to clients for the next round
34: end for
```

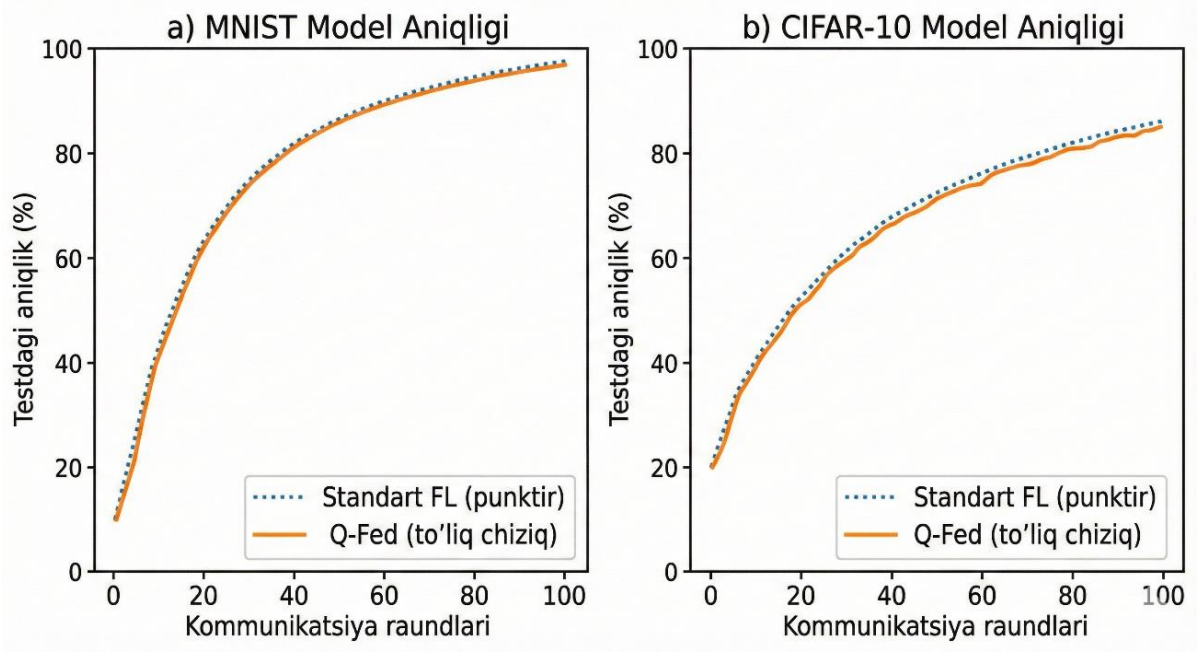
Eksperimental o‘rnatish (Experimental Setup):

- **Dasturiy ta'minot:** Simulyatsiyalar Python 3.9, PyTorch 1.12 (ML modellari uchun) va liboqs kutubxonasining Python interfeysi (PQC algoritmlari uchun) yordamida amalga oshirildi.
- **Ma'lumotlar to‘plamlari:** Biz ikkita standart ma'lumotlar to‘plamidan foydalandik:
- **MNIST:** Qo‘lda yozilgan raqamlarning 60,000 ta o‘quv va 10,000 ta test tasvirlari.
- CIFAR-10: 10 ta sinfga oid 60,000 ta rangli tasvirlar.
- Ma'lumotlar 100 ta mijoz o‘rtasida mustaqil va bir xil taqsimlangan (IID) holda bo‘lindi.
- **Model arxitekturasi:** MNIST uchun ikkita konvolyutsion qatlamli oddiy CNN va CIFAR-10 uchun biroz murakkabroq CNN modeli ishlatildi.
- **Baholash mezonlari:**
- **Model aniqligi (Accuracy):** Test ma'lumotlar to‘plamidagi global modelning aniqligi.
- **Hisoblash vaqti (Computation Time):** Bir raunddagi shifrlash, deshifrlash va imzolash/tekshirish uchun ketgan o‘rtacha vaqt (ms).
- **Kommunikatsiya xarajatlari (Communication Overhead):** Shifrlangan va imzolanagan yangilanishning hajmi (KB).

NATIJALAR (RESULTS)

Eksperimentlarimiz Q-Fed arxitekturasining amaliy samaradorligini va xavfsizlik uchun to‘lanadigan "narxini" baholashga qaratildi.

Model aniqligi: Eng muhim natijalardan biri shuki, Q-Fed arxitekturasi modelning o‘rganish jarayoniga deyarli hech qanday salbiy ta'sir ko‘rsatmadi. 1-rasmda ko‘rsatilganidek, ham standart FL, ham Q-Fed uchun model aniqligining o‘sish egri chiziqlari deyarli bir xil. Bu bizning yondashuvimiz xavfsizlikni oshirish bilan birga, modelning asosiy vazifasiga putur yetkazmasligini isbotlaydi.



Rasm 2. : Standart FL va Q-Fed arxitekturalarining model aniqligi bo‘yicha solishtirma tahlili.

Jadval 1.

Standart FL va Q-Fed ning unumdorlik ko‘rsatkichlari (MNIST modeli uchun, bir mijozga hisoblanganda)

Ko‘rsatkich	Standart FL (himoyasiz)	Q-Fed (Kyber+Dilithium)	Farq (%)
Shifrlash/Imzolash vaqti (mijoz, ms)	~0	15.8	+∞
Deshifrlash/Tekshirish vaqti (server, ms)	~0	21.2	+∞
Yangilanish hajmi (KB)	545 KB	551.2 KB	+1.1%
Umumiy raund vaqti (qo‘shimcha, ms)	**0**	**~37 ms**	**-**

Jadvaldan ko‘rinib turibdiki, PQC operatsiyalari uchun sarflanadigan vaqt millisekundlarda o‘lchanadi. Bir qarashda bu kichik ko‘rinsa-da, minglab mijozlar ishtirok etadigan katta hajmli tizimlarda bu qo‘shimcha xarajatlar sezilarli bo‘lishi mumkin. Kommunikatsiya xarajatlarining ortishi esa nisbatan kichik – atigi 1.1% atrofida, chunki PQC kalitlari va imzolari model og'irliklarining umumiy hajmiga nisbatan ancha kichik.

MUHOKAMA (DISCUSSION)

Olingan natijalar bir nechta muhim xulosalarni taqdim etadi. Birinchidan, federativ ta'lim tizimlarini post-kvant kriptografiyasi yordamida himoya qilish nafaqat nazariy jihatdan mumkin, balki amaliy jihatdan ham realdir. Q-Fed arxitekturasi model unumdorligiga ta'sir qilmasdan, kelajakdagi kvant tahdidlariga qarshi mustahkam himoyani ta'minlay oladi.

Ikkinchidan, asosiy muvozanat – **xavfsizlik va unumdorlik** o‘rtasida yotadi. Bizning tahlilimiz shuni ko‘rsatadiki, kvant-barqarorlik uchun to‘lov – bu qo‘shimcha hisoblash vaqti. Har bir raundga qo‘shilgan ~37 ms vaqt real vaqtda ishlaydigan yoki resurslari cheklangan qurilmalar (masalan, IoT) uchun muhim bo‘lishi mumkin. Bu, o‘z navbatida, kelajakda PQC algoritmlarini apparat darajasida tezlashtirish (hardware acceleration) zarurligini ko‘rsatadi.

Ushbu tadqiqotning amaliy ahamiyati, ayniqsa, O‘zbekiston kabi raqamli iqtisodiyotni faol rivojlantirayotgan mamlakatlar uchun yuqori. Mamlakatimizda "Click", "Payme" kabi raqamli to‘lov tizimlarining ommalashishi, bank sohasida sun'iy intellektga asoslangan firibgarlikni aniqlash tizimlarining joriy etilishi shaxsiy moliyaviy ma'lumotlar xavfsizligini birinchi o‘ringa olib chiqadi. Q-Fed kabi arxitekturalar ushbu tizimlarni nafaqat bugungi, balki ertangi kun tahdidlaridan ham himoya qilish imkonini beradi.

Tadqiqotning cheklovlari. Ushbu ish bir qator cheklovlarga ega. Birinchidan, barcha eksperimentlar ideal tarmoq sharoitlarida simulyatsiya qilindi. Real hayotdagi tarmoq kechikishlari va uzilishlar tizimning umumiy unumdorligiga ta'sir qilishi mumkin. Ikkinchidan, biz faqat IID ma'lumotlar taqsimotini ko‘rib chiqdik. Non-IID holatlari model konvergentsiyasiga qanday ta'sir qilishini o‘rganish alohida tadqiqotni talab etadi. Uchinchidan, biz faqat bitta turdagi PQC algoritmlarini (panjaraga asoslangan) tahlil qildik.

Kelajakdagi ishlar. Kelajakda ushbu tadqiqotni bir necha yo‘nalishda kengaytirish mumkin: (a) turli PQC oilalariga mansub algoritmlarning samaradorligini solishtirish; (b) resurslari cheklangan qurilmalar uchun yengillashtirilgan PQC protokollarini ishlab chiqish; (c) Q-Fed arxitekturasini zaharlash va boshqa turdagi hujumlarga qarshi himoya mexanizmlari bilan birlashtirish.

XULOSA (CONCLUSION)

Biz ma'lumotlar maxfiyligi va kvant hisoblashlari davrida federativ ta'lim tizimlarining xavfsizligini ta'minlashga qaratilgan Q-Fed arxitekturasini taklif etdik. Post-kvant kriptografiyasini FL jarayoniga muvaffaqiyatli integratsiya qilib, biz model aniqligini saqlagan holda kvant-barqaror xavfsizlikka erishish mumkinligini ko‘rsatdik. Garchi bu yondashuv ma'lum bir hisoblash xarajatlarini talab qilsa-da, u maxfiylik muhim bo‘lgan sohalarda – sog'liqni saqlash, moliya va kritik infratuzilmalarda – ishonchli va kelajakka mo‘ljallangan AI tizimlarini qurish uchun mustahkam poydevor yaratadi. Ushbu ish sun'iy intellekt va kiberxavfsizlikning kesishuvidagi muhim tadqiqot yo‘nalishiga o‘z hissasini qo‘shadi.

ADABIYOTLAR RO‘YXATI (REFERENCES)

1. Shlezinger, A., & Shlezinger, M. (2020). The New AI: The Future of Artificial Intelligence is Here. Apress.
2. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS).
3. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.
4. Alagic, G., et al. (2020). Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST Internal Report 8309.
5. Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. (2020). Federated Optimization in Heterogeneous Networks. Proceedings of the Conference on Machine Learning and Systems (MLSys).
6. Bhagoji, A. N., Chakraborty, S., Mittal, P., & Calo, S. (2019). Analyzing Federated Learning through Poisoning Attacks. arXiv preprint arXiv:1911.11835.
7. Zhu, L., Liu, Z., & Han, S. (2019). Deep Leakage from Gradients. Advances in Neural Information Processing Systems (NeurIPS), 32.
8. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
9. Yin, X., et al. (2021). A Post-Quantum Secure Federated Learning Framework. 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).
10. Ducas, L., Lyubashevsky, V., & Prest, T. (2018). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. 2018 IEEE European Symposium on Security and Privacy (EuroS&P).
11. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Schanck, G., & Stehle, D. (2018). CRYSTALS-Dilithium: a lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238-268.
12. Kairouz, P., et al. (2021). Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning, 14(1–2), 1-210.