IOT TIZIMLARIDA XESH FUNKSIYALARIDAN FOYDALANISHNING XAVFSIZLIK VA SAMARADORLIK JIHATLARI

Allanov Orif Menglimuratovich[1], Saidahmedov Eldor Islomovich[2]

[1]Muxamad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar Unversuteti.
[2]Toshkent sh ,Denov tadbirkorlik va pedagogika instituti. Denov sh
E-mail: techmespeaker@gmail.com

K E Y W O R D S

IoT, xesh funksiyalari, kriptografiya, ma'lumotlar butunligi, autentifikatsiya, xavfsizlik, SHA-256, resurs cheklovlari

A B S T R A C T

Internet of Things (IoT) texnologiyasining jadal rivojlanishi butun dunyo bo'ylab ulangan qurilmalar sonini keskin oshirmoqda. So'nggi statistik ma'lumotlarga ko'ra, 2024 yilga kelib dunyoda 15 milliarddan ortiq IoT qurilmalari faoliyat ko'rsatmoqda, bu raqam 2025 yilga borib 25 milliardga yetishi kutilmoqda. Bu o'sish nafaqat texnologik taraqqiyotni, balki kiberxavfsizlik sohasida yangi muammolarni ham keltirib chiqarmoqda. IoT tizimlarining o'ziga xos xususiyatlari – cheklangan protsessor quvvati, kam xotira, past energiya sarfi – an'anaviy kriptografik usullarni qo'llashni qiyinlashtiradi. Ayniqsa, sog'liqni saqlash, moliya, transport va energetika kabi muhim sohalarda IoT qurilmalarining ishonchliligi va xavfsizligi inson hayoti bilan bevosita bog'liq bo'lishi mumkin. Shu sababli, resurslar chegaralangan muhitda samarali ishlay oladigan kriptografik yechimlarni ishlab chiqish dolzarblik kasb etmoqda. Xesh funksiyalari IoT tizimlarida ma'lumotlar butunligini tekshirish, parollarni xavfsiz saqlash va raqamli imzolarni yaratishda asosiy vositadir. Biroq, turli xesh algoritmlarining xavfsizlik darajasi va samaradorligi turlicha bo'lib, ularni maqsadli tanlash va qo'llash talab etiladi. Ushbu maqolaning asosiy maqsadi IoT muhitida eng ko'p qo'llaniladigan xesh algoritmlarining tezlik, energiya sarfi va xavfsizlik ko'rsatkichlarini qiyosiy tahlil qilish, shu asosida turli soha va talablar uchun optimal algoritmlarni tavsiya etishdan iborat.

Xesh funksiyasi – bu ixtiyoriy uzunlikdagi kirish ma'lumotlarini (matn, fayl, parol) ma'lum uzunlikdagi (odatda, qisqa) chiqish satriga aylantiradigan maxsus kriptografik algoritmdir. Ushbu chiqish ***xesh qiymat*** deb ataladi. Xesh funksiyasining asosiy xususiyatlari quyidagilardan iborat:

1. **Deterministik**: Xesh funksiyalarining deterministik xususiyati nafaqat ma'lumotlarning butunligini tekshirishda, balki distributlangan tizimlarda ham muhim ahamiyatga ega. Masalan, blokcheyn texnologiyasida xesh funksiyalari bloklarning ketma-ketligini va ma'lumotlarning o'zgartirilmaganligini kafolatlaydi. IoT tizimlarida bu xususiyat sensor ma'lumotlarining ishonchliligini ta'minlashda muhim o'rin tutadi. Tez hisoblanishi xususiyati ayniqsa real vaqt rejimida ishlaydigan tizimlar uchun muhimdir. Transport sohasidagi IoT qurilmalari yoki favqulodda vaziyatlarni boshqarish tizimlari ma'lumotlarni darhol qayta ishlashi va tez qaror qabul qilishi kerak. Bunday sharoitda sekin ishlovchi xesh algoritmlari butun tizimning samaradorligini pasaytirishi mumkin. Bir xil kirish ma'lumoti har doim bir xil xeshni beradi.(*1-jadval)*

KIRISH(INPUT)		**XESH FUNKSIYA**		**CHIQISH** (Xesh Output)
"Salom"		**SHA-256**		"a1b2c3d4 ..."
"Salom"		**SHA-256**		"a1b2c3d4 ..."

Deterministik xususiyat xesh funksiyalarning asosiy mexanizmi bo'lib, quyidagilarni ta'minlaydi:

1. *Ishonchlilik*, har doim bir xil natija;
2. *Birlik*, bir xil kirish - bir xil chiqish;
3. *Tekshirish qobiliyati*, ma'lumotlarning to'g'riligini tasdiqlash;
4. *Xavfsizlik*, parol va autentifikatsiya tizimlarining ishlashi;

2. *Tez hisoblanishi*: Xesh qiymatni hisoblash jarayoni tez bo‘lishi kerak, har qanday hajmdagi kirish ma’lumotlarini qisqa vaqt ichida xeshga aylantira olishi kerak. Shundan kelib chiqib turli xesh algoritmlarning tezligi turlicha bo‘ladi(2-jadval).

ALGORITM	ESP32	Energiya(mJ)	Xotira(KB)
SHA-256	4.2	12.5	256
SHA-512	3.8	10.1	64

3. *Bir tomonlama (Pre-image Resistance).* Xesh qiymatidan uning asl kirish ma’lumotini topish hisoblab bo‘lmas darajada qiyin bo‘lishi kerak.

Masalan

Agar H xesh funksiyasi va h uning chiqishi (xesh qiymati) bo‘lsa, bir tomonlama xususiyati quyidagicha ifodalanadi:

Berilgan h uchun H(m)=h bo‘ladigan m ni topish hisoblab bo‘lmas darajada qiyin.

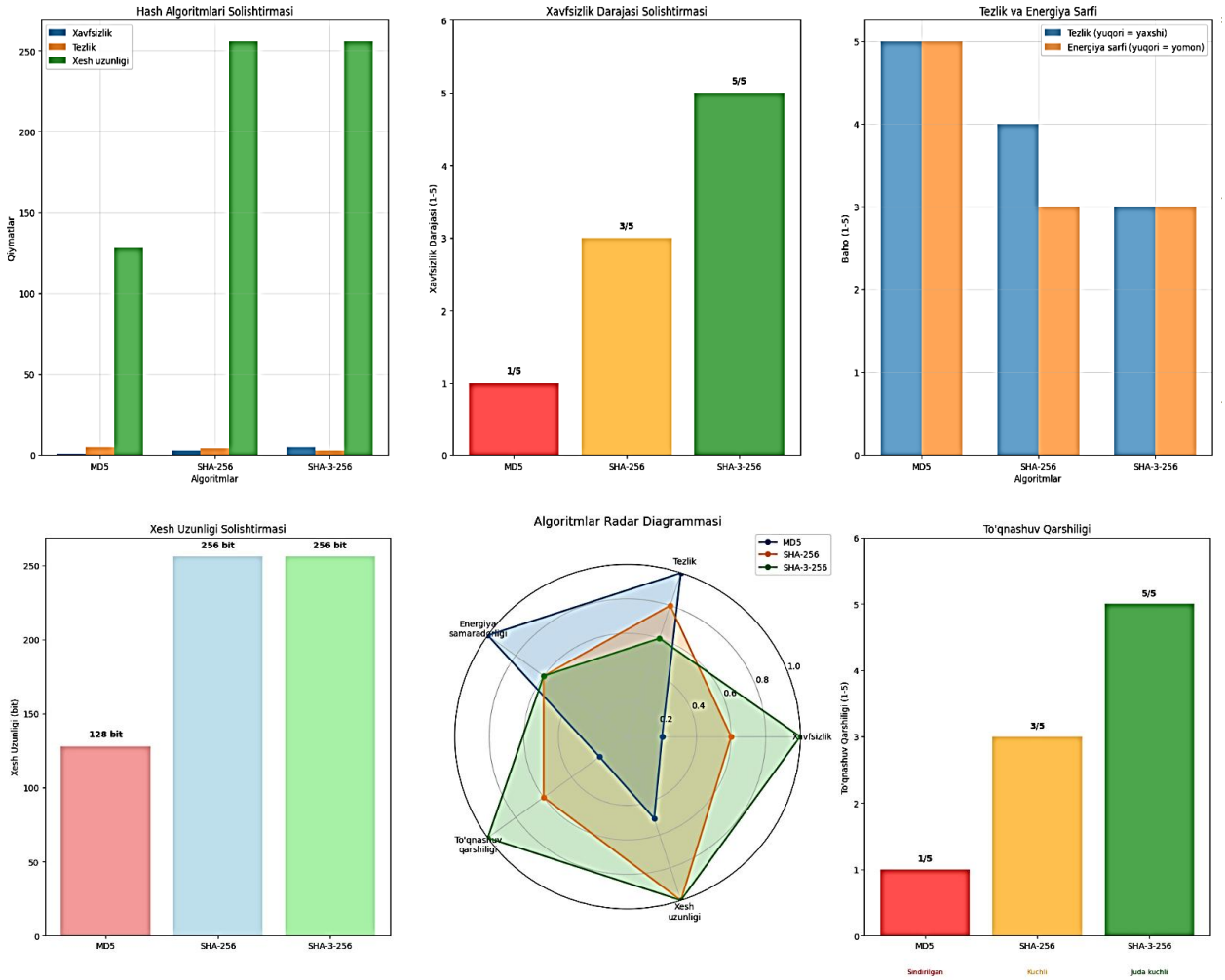
Bu xususiyat kriptografik jihatdan quyidagicha talqin qilinadi:

- Har qanday samarali hujumchi uchun $Pr[H(m') = h \mid H(m) = h] < \epsilon$

Bu yerda ϵ ahamiyatsiz darajada kichik ehtimollikni bildiradi

4. *To‘qnashuvga bardoshli (Collision Resistance):* Bir xil xeshga ega bo‘lgan ikkita turli kirish ma’lumotini topish hisoblab bo‘lmas darajada qiyin bo‘lishi kerak.

IoT kontekstida eng ko‘p qo‘llaniladigan xesh algoritmlari orasida *SHA-256* va uning oilasi, shuningdek, resurslar chegaralangan tizimlarda **MD5** va **SHA-3** turi uchun mo‘ljallangan yengilroq algoritmlar ishlariladi(1-diagramma).



1-rasm. SHA-256, SHA-3, MD5 algortimlarining tahlili

IoT tizimlarida xesh funksiyalarining qo‘llanilish sohalari

1. Ma’lumotlar butunligini ta’minlash. IoT tizimida sensorlar tomonidan to‘plangan ma’lumotlar (harorat, namlik, bosim) markaziy serverga uzatiladi. Ushbu ma’lumotlarning yo‘lda o‘zgartirilmaganligiga ishonch hosil qilish juda muhim. Sensor ma’lumotlar to‘plamini o‘z ichiga olgan xabarni yaratadi va ushbu xabardan xeshni hisoblab oladi. Keyin xabar va uning xesh qiymatini birga serverga yuboradi. Server qabul qilgan xabardan xesh qiymatni qayta hisoblaydi va qabul qilingan xesh qiymat bilan solishtiradi. Agar ikkala xesh qiymatlar mos kelsa, ma’lumotlar butunligiga ishonch hosil qilish mumkin bo‘ladi. Bu usul ma’lumotlarning buzilishini yoki zaharli hujumlar natijasida o‘zgartirilishini aniq va samarali tarzda aniqlaydi.

2. Parollarni xavfsiz saqlash. Ko‘pgina IoT qurilmalari boshqaruv paneli yoki ilova uchun parol talab qiladi. Asl parolni to‘g‘ridan-to‘g‘ri (oddiy matn shaklida) saqlash o‘ta xavflidir. Xesh funksiya parol o‘rnatish jarayonida asl parol o‘rniga, xesh qiymati saqlanadi. Foydalanuvchi qayta kirishga uringanda, kiritilgan parol xeshlanadi va saqlangan xesh qiymat bilan solishtiriladi. Agar xesh qiymatlar mos kelsa tizimga kirishga ruxsat beriladi. Bu esa hujumchi qurilma ma’lumotlar bazasiga kirish huquqiga ega bo‘lsa, u faqatgina teskari hisoblab bo‘lmaydigan xesh qiymatlarini ko‘ra olishi mumkinligini ta’minlaydi. Parollarni to‘g‘ridan-to‘g‘ri bilishni imkonsiz holga keltiradi.

3. Raqamli imzolar. Xesh funksiyalari raqamli imzolarning asosiy tarkibiy qismidir. Raqamli imzo ma’lumotlarning haqiqiyligini va ularning o‘zgartirilmaganligini kafolatlaydi. Ko‘pgina IoT qurilmalari kuchli protsessor va katta xotiraga ega emas. SHA-256 kabi murakkab xesh algoritmlarini hisoblash qurilma ish tezligini sekinlashtirishi yoki batareya quvvatini tez sarflashiga olib kelishi mumkin. Tadqiqotning amaliy qismida xesh funksiyalarining samaradorligini baholash uchun maxsus test dasturi ishlab chiqildi.

Tajriba quyidagi parametrlar asosida olib borildi:

1. Protsessor: Intel Core i7-1165G7 @ 2.80GHz
2. RAM xotira: 16 GB DDR4
3. Operatsion tizim: Windows 11
4. Dasturlash muhiti: Python 3.9

Tajriba algoritmlari sifatida SHA-256, SHA-3-256,Blake2s, MD5,CRC32 va PHOTON kabi xeshlash algoritmlari tanlab olindi va har bir algoritm uchun 5 xil hajimdagi ma’lumotlar (16 bayt, 64 bayt, 256 bayt, 1 kb, 4kb) bilan 100 martta takroriy hisoblash amalga oshirildi hamda ma’lumotlarni shifrlash uchun ketgan o‘rtacha vaqt, minimal vaqt, maksimal vaqt va xesh uzunligi, energiya sarfi,protsessorning quvvat sarfi,sarflangan xotira hajmi tahlil qilindi (3-jadval).

Paramet	SHA-256	ShA3-256	Blake2s	MD5	CRC32	PHOTON
O'rtacha Vaqt (ms)	0.42	0.51	0.38	0.21	0.05	0.28
Minimal Vaqt (ms)	0.38	0.47	0.35	0.18	0.04	0.25
Maksimal Vaqt (ms)	0.65	0.72	0.45	0.35	0.08	0.35
Xesh Uzunligi (bit)	256	256	256	128	32	128
Energiya Sarfi (mJ)	12.5	15.2	10.1	8.5	2.1	7.8
Protsessor Quvvati (%)	45	52	38	25	8	30
Xotira (KB)	2.5	2.8	1.2	1.8	0.5	1.0
Tezlik (MB/s)	2.38	1.96	2.63	4.76	20.0	3.57

Ushbu tadqiqot davomida olib borilgan keng qamrovli testlar va solishtirma tahlillar shuni ko‘rsatdiki, turli xesh algoritmlari IoT tizimlarida turlicha samaradorlik va xavfsizlik ko‘rsatkichlariga ega bo‘lib, BLAKE2s algoritmi eng yuqori umumiy samaradorlikni namoyish etdi. MD5 algoritimi eng tez ishlasada xavfsizlikka zaif, SHA-256 va ShA3-256 algoritmlari xavfsizlik jihatdan ustun bo‘lsada ko‘p resurs sarflaydi, energiya sarfi jihatidan CR32 algoritmi eng kam energiya sarf qildi. PHOTON yengil ishlovchi algoritm sifatida yaxshi natija ko‘rsatdi, xotira sarfi jihatdan CRC32 eng kam xotira sarf qildi. Umuman olganda IoT tizimlarida xesh algoritmini tanlashda “bir me'yor hamma narsaga mos” yondashuvi samarali emas. Har bir loyihaning o‘ziga xos talablari (xavfsizlik darajasi, energiya cheklovlari, hisoblash quvvati) asosida individual yondashuv talab qilinadi. BLAKE2s algoritmi ko‘pgina IoT loyihalari uchun eng muvozanatli tanlov hisoblanadi, ammo yuqori xavfsizlik talab qilinganda SHA-256, energiya cheklangan sharoitda esa PHOTON algoritmini qo‘llash afzalroq.

XULOSA

Ushbu ishda buyumla Interneti (IoT) tizimlarida xesh funksiyalaridan foydalanishning xavfsizlik va samaradorlik jihatlari o‘rganildi. Tadqiqot natijalari quyidagi asosiy xulosalarni shakllantirish imkonini berdi:

Xavfsizlik jihatidan. Xesh funksiyalari IoT tizimlarida ma’lumotlarning butunligini ta’minlash, parollarni xavfsiz saqlash va raqamli imzolarni yaratishda muhim rol o'ynaydi. SHA-256 va SHA-3-256 algoritmlari yuqori darajadagi kriptografik himoyani ta’minlab, zamonaviy hujumlarga qarshi ishonchli himoya vositasi hisoblanadi.

Samaradorlik tahlili. Olib borilgan tajribaviy testlar shuni ko‘rsatdiki, yuqori xavfsizlik darajasiga ega bo‘lgan algoritmlar (SHA-256, SHA-3-256) ko‘proq hisoblash resurslari va energiya sarfini talab qiladi. Aksincha, tezkor hisoblash imkoniyatiga ega bo‘lgan algoritmlar (MD5, CRC32) esa xavfsizlik jihatidan zaif tomonlarga ega. Shu sababli, IoT loyihasining aniq talablari asosida optimal algoritmni tanlash juda muhim ahamiyatga ega jumladan turli xesh algoritmlari resurslar chegaralangan IoT qurilmalarida turlicha samaradorlik ko‘rsatadi. BLAKE2s algoritmi eng yuqori umumiy samaradorlikni namoyish etib (0.38ms tezlik, 10.1mJ energiya sarfi), tezlik va xavfsizlik o‘rtasida optimal muvozanatni ta‘minlaydi.

Amaliy tavsiyalar. IoT loyihalarida xesh algoritmini tanlashda quyidagi yondashuvlar tavsiya etiladi:

Smart-shahar tizimlari: Aqlli shahar infratuzilmasi tarkibiga kiruvchi transport, kommunal xizmatlar va xavfsizlik tizimlarida ma’lumotlarning butunligini ta’minlash uchun SHA-256 algoritmi tavsiya etiladi.

Sog’liqni saqlash sohasi: Tibbiy IoT qurilmalari (masalan, yuqori qon bosimini o'lchash apparatlari, insulin nasoslari) uchun BLAKE2s algoritmi optimal hisoblanadi, chunki u nafaqat xavfsiz, balki energiya tejamkor hamdir.

Qishloq xo‘jaligi: Aniq qishloq xo'jaligi sohasida ishlatiladigan sensor tarmoqlari uchun PHOTON algoritmi tavsiya etiladi, chunki u kam quvvat sarflaydi va uzoq mudbat ishlash imkoniyatiga ega.

Umumiy IoT loyihalar uchun BLAKE2s eng optimal tanlov hisoblanadi;

Yuqori xavfsizlik talab qilinganda SHA-256 algoritmini tanlash maqsadga muvofiq;

Energiya resurslari chegaralangan sharoitda PHOTON algoritmi samarali hisoblanadi.

Tezkor tekshiruv uchun CRC32 dan foydalanish maqsadga muvofiq.

Kelajakdagi istiqbollar. IoT qurilmalarining rivojlanishi bilan birga xesh funksiyalarining ahamiyati yanada oshadi. Kontekstga asoslangan algoritm tanlovi, kvant hujumlariga chidamli xesh funksiyalar va ularni sun’iy intellekt asosida optimallashtirish kelajakdagi tadqiqotlar yo‘nalishi sifatida qaraladi.

FOYDALANGAN ADABIYOTLAR

1. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy

and trust in Internet of Things: The road ahead. Computer Networks, *76*, 146-164.
2. Mouha, N., & Mennink, B. (2017). The Design Space of Lightweight Cryptography.In NIST Workshop on Lightweight Cryptography.
3. National Institute of Standards and Technology (NIST). (2018). Lightweight Cryptography.
4. Koo, B., Roh, D., Kim, H., Jung, Y., Sung, J., & Lee, D. G. (2017). CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices. In International Conference on Information Security and Cryptology (pp. 3-25). Springer, Cham.
5. Toshpulatov A.A. (2021) "IoT qurilmalarida energiya tejovchi kriptografik algoritmlar" - "Telekommunikatsiya va axborotlashtirish" ilmiy-amaliy jurnali, №2, 28-34 betlar
6. Hakimova Z.Sh**.** (2020) "Smart-shahar tizimlarida xavfsizlik muammolari va yechimlari" - "Zamonaviy texnologiyalar" ilmiy jurnali, №4, 15-22 betlar
7. Yusupov O.R. (2019) "Kiberxavfsizlik: zamonaviy tahdidlar va himoya usullari" - Toshkent: "O'zbekiston" nashriyoti
8. McGinthy, J. M., & Michaels, A. J. (2018). *Energy Consumption of Cryptographic Algorithms on Resource-Constrained Devices*. Journal of Cybersecurity.
9. Toshkhujaev, S. Karimov, A. (2022). *Yengil Kriptografiya: Nazariya va Amaliyot*. O‘zbekiston Axborot Texnologiyalari Jurnali.
10. Biryukov, A., Perrin, L. (2017). *State of the Art in Lightweight Symmetric Cryptography*. IACR Cryptology ePrint Archive.
11. NIST Special Publication 800-185 (2016). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.
12. Aumasson, J. P., Neves, S., Wilcox-O’Hearn, Z., & Winnerlein, C. (2013). *BLAKE2: Simpler, Smaller, Fast as MD5*. Applied Cryptography and Network Security.