OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“YENGIL VAZNLI KRIPTOGRAFIYA”
MODULI BO‘YICHA
O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

OLIY TA’LIM TIZIMI PEDAGOG VA RAHBAR KADRLARINI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISHNI TASHKIL ETISH BOSH ILMIY - METODIK MARKAZI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“Kriptologiya” yo‘nalishi

“YENGIL VAZNLI KRIPTOGRAFIYA”
MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

Modulning o‘quv-uslubiy majmuasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024 yil 27 dekabrdagi №485-sonli buyrug‘i bilan tasdiqlangan o‘quv dasturi va o‘quv rejasiga muvofiq ishlab chiqilgan.

Tuzuvchilar: **Z.T.Xudoykulov -** PhD, dotsent

Taqrizchilar: **B.F. Abdurahimov** – fizika-matematika fanlari doktori, professor.
O.P. Axmedova - texnika fanlari nomzodi, dotsent.

O‘quv-uslubiy majmua O‘quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining qarori bilan tasdiqqa tavsiya qilingan (2024-yil 27-noyabrdagi 3/4 (745/746)- sonli bayonnoma).

MUNDARIJA

I BO‘LIM.
ISHCHI DASTUR

I. ISHCHI DASTUR

KIRISH

Ushbu dastur O‘zbekiston Respublikasining 2020-yil 23-sentabrda tasdiqlangan “Ta’lim to‘g‘risida” Qonuni, O‘zbekiston Respublikasi Prezidentining 2015-yil 12-iyundagi “Oliy ta’lim muassasalarining rahbar va pedagog kadrlarini qayta tayyorlash va malakasini oshirish tizimini yanada takomillashtirish to‘g‘risida” PF-4732-son, 2019-yil 27-avgustdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to‘g‘risida” PF-5789-son, 2019-yil 8-oktabrdagi “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida” PF-5847-son, 2020-yil 29-oktabrdagi “Ilm-fanni 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida” PF-6097-son, 2022-yil 28-yanvardagi “2022-2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida” PF-60-son, 2023-yil 25-yanvardagi “Respublika ijro etuvchi hokimiyat organlari faoliyatini samarali yo‘lga qo‘yishga doir birinchi navbatdagi tashkiliy chora-tadbirlar to‘g‘risida” PF-14-son, O‘zbekiston Respublikasi Prezidentining 2023-yil 11-sentabrdagi ““O‘zbekiston — 2030” strategiyasi to‘g‘risida” PF-158-son Farmonlari, shuningdek, 2024-yil 15-avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-son Qarori, shuningdek, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2019-yil 23-sentabrdagi “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining malakasini oshirish tizimini yanada takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi 797-son Qarori hamda O‘zbekiston Respublikasi Vazirlar Mahkamasining “Oliy ta’lim tashkilotlari rahbar va pedagog kadrlarini qayta tayyorlash va malakasini oshirish tizimini samarali tashkil qilish chora-tadbirlari to‘g‘risida” 2024-yil 11-iyuldagi 415-son Qarorlarida belgilangan ustuvor vazifalar mazmunidan kelib chiqqan holda tuzilgan bo‘lib, u oliy ta’lim muassasalari pedagog kadrlarining kasb mahorati hamda innovatsion kompetentligini rivojlantirish, sohaga oid ilg‘or xorijiy tajribalar, yangi bilim va malakalarni o‘zlashtirish, shuningdek amaliyotga joriy etish ko‘nikmalarini takomillashtirishni maqsad qiladi.

Qayta tayyorlash va malaka oshirish yo‘nalishining o‘ziga xos xususiyatlari hamda dolzarb masalalaridan kelib chiqqan holda dasturda tinglovchilarning ushbu fan doirasidagi bilim, ko‘nikma, malaka hamda kompetensiyalariga qo‘yiladigan talablar takomillashtirilishi mumkin.

Modulning maqsadi va vazifalari

Modulining maqsadi: hisoblash, quvvat, tarmoq imkoniyatlari cheklangan hisoblash muhitida ishlashga mo‘ljallangan (yengil vaznli) kriptografik algoritmlar,

ularni loyihalash tartibi, kriptotahlili haqida oliy ta’lim muassasalari pedagog kadrlarining bilim, ko‘nikma va malakalarini oshirish.

Modulning vazifalari:

- Imkoniyati cheklangan muhitlar, ularda ishlovchi qurilmalarning tavsifi va tasnifi,
- Yengil vaznli kriptografik algoritmlarni yaratishdagi yondashuvlar, loyihalash asoslari,
- Zamonaviy yengil vaznli kriptografik algoritmlar,
- Zamonaviy yengil vaznli kriptografik algoritmlarning kriptotahlil natijalari, algoritmlarni dasturiy amalga oshirish haqida nazariy va amaliy bilimlarni, ko‘nikma va malakalarni shakllantirishdan iborat.

Modul bo‘yicha tinglovchilarning bilim, ko‘nikma, malaka va kompetensiyalariga qo‘yiladigan talablar

“Yengil vaznli kriptografiya” modulini o‘zlashtirish jarayonida amalga oshiriladigan masalalar doirasida:

Tinglovchi:

Imkoniyati cheklangan qurilmalar, ularning tasnifi, apparat va dasturiy ta’minotini;

Yengil vaznli kriptografik algoritmlar, ularni qurishdagi yondashuvlarni;

Zamonaviy yengil vaznli kriptografik algoritmlarning ishlash tartibini;

Zamonaviy kriptografik algoritmlarning kriptotahlil natijalarini ***biladi***.

Yengil vaznli kriptografik algoritmlarni tahlillash, turli akslantirishlarni samaradorlik va xavfsizlik bo‘yicha baholay olish, yengil kriptografik algoritmlardan amalda foydalana olishi ***ko‘nikmalariga*** ega bo‘ladi.

Turli imkoniyati cheklangan muhitlar uchun mos kriptografik algoritmlarni yaratish, kriptografik algoritmlarni dasturiy va apparat tomonlama amalga oshirish ***malakalariga*** ega bo‘ladi.

Modulni tashkil etish va o‘tkazish bo‘yicha tavsiyalar

“Yengil vaznli kriptografiya” moduli ma’ruza va amaliy mashg‘ulotlar shaklida olib boriladi.

Modulni o‘qitish jarayonida ta’limning zamonaviy metodlari, pedagogik texnologiyalar va axborot-kommunikatsiya texnologiyalari qo‘llanilishi nazarda tutilgan:

- ma’ruza darslarida zamonaviy kompyuter texnologiyalari yordamida prezentatsion va elektron-didaktik texnologiyalardan;
- o‘tkaziladigan amaliy mashg‘ulotlarda texnik vositalardan, ekspress-so‘rovlar, test so‘rovlari, aqliy hujum, guruhli fikrlash, kichik guruhlar bilan ishlash, kollokvium o‘tkazish, va boshqa interaktiv ta’lim usullarini qo‘llash nazarda tutiladi.

Modulning o‘quv rejadagi boshqa modullar bilan bog‘liqligi va uzviyligi

“Yengil vaznli kriptografiya” moduli mazmuni o‘quv rejadagi “Kriptografiyaning matematik asosi”, “Zamonaviy kriptotahlil usullari” o‘quv modullari bilan uzviy bog‘langan holda pedagoglarning ta’lim jarayonida kriptologiya sohasini chuqur o‘rgatishga xizmat qiladi.

Modulning oliy ta’limdagi o‘rni

Modulni o‘zlashtirish orqali tinglovchilar ta’lim jarayonida turli imkoniyati cheklangan muhitlar uchun kriptografik algoritmlarni loyihalash, tanlash va kriptotahlil usullariga baholash bo‘yicha kasbiy kompetentlikka ega bo‘ladilar.

MODUL BO‘YICHA SOATLAR TAQSIMOTI

№	Modul mavzulari	Auditoriya uquv yuklamasi				
		Jami	jumladan			
			Nazariy	Amaiy mashg‘ulot	Ko‘chma mashg‘uloti	
1.	**Yengil vaznli kriptografiya (YVK):** IoT va uning qurilmalari, ularni hisoblash imkoniyatlari, ananaviy kriptografik algoritmlarni amalga oshirishdagi muammolar, xavfsizlik muammolari. Himoya mexanizmlari.	2	2			
2.	**Yengil vaznli kriptografik algoritmlar:** simmetrik kalitli, ochiq kalitli kriptografik algoritmlar, xesh funksiyalar, gamomorfik shifrlash usullari, kriptografik kalitlarni boshqarish, kriptografik protokollar.	2	2			
3.	**Yengil vaznli kriptografiya bo‘yicha NIST konkursi:** talablar, o‘tkazilish bosqichlari, ishtirokchi algoritmlar, ASCON algoritmi.	6	2	4		
4.	**Yengil vaznli kriptografik algoritmlarni qurish, samarali apparat va dasturiy amalga oshirish**	6	2	4		

	usullari: YVK algoritmlarni qurish usullari, S jadvalni tanlash, amalga oshirish usullari, chiziqli akslantirishlarni tanlash va amalga oshirish, raundlar sonini tanlash.					
	Jami:	**16**	**8**	**8**		

NAZARIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: YENGIL VAZNLI KRIPTOGRAFIYA (YVK) (2 SOAT)

IoT va uning qurilmalari, ularni hisoblash imkoniyatlari, ananaviy kriptografik algoritmlarni amalga oshirishdagi muammolar, xavfsizlik muammolari. Himoya mexanizmlari.

2-MAVZU: YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLAR (2 SOAT).

Simmetrik kalitli, ochiq kalitli kriptografik algoritmlar, xesh funksiyalar, gamomorfik shifrlash usullari, kriptografik kalitlarni boshqarish, kriptografik protokollar.

3-MAVZU: YENGIL VAZNLI KRIPTOGRAFIYA BO‘YICHA NIST KONKURSI (2 SOAT).

Talablar, o‘tkazilish bosqichlari, ishtirokchi algoritmlar, ASCON algoritmi.

4-MAVZU: YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLARNI QURISH, SAMARALI APPARAT VA DASTURIY AMALGA OSHIRISH USULLARI (2 SOAT).

YVK algoritmlarni qurish usullari, S jadvalni tanlash, amalga oshirish usullari, chiziqli akslantirishlarni tanlash va amalga oshirish, raundlar sonini tanlash.

AMALIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: ASCON ALGORITMI (4 SOAT)

Ascon algoritmini dasturiy ko‘rinishga amalga oshirish.

2-MAVZU: PRESENT ALGORITMNI (4 SOAT)

PRESENT algoritmni apparat va dasturiy ko‘rinishda amalga oshirish.

KO‘CHMA MASHG‘ULOT MAZMUNI

Ushbu modul bo‘yicha ko‘chma mashg‘ulotlar nazarda tutilmagan.

O‘QITISH SHAKLLARI

Mazkur modul bo‘yicha quyidagi o‘qitish shakllaridan foydalaniladi:

- ma’ruzalar, amaliy mashg‘ulotlar (ma’lumotlar va texnologiyalarni anglab olish, motivatsiyani rivojlantirish, nazariy bilimlarni mustahkamlash);
- davra suhbatlari (ko‘rilayotgan loyiha yechimlari bo‘yicha taklif berish qobiliyatini rivojlantirish, eshitish, idrok qilish va mantiqiy xulosalar chiqarish);

bahs va munozaralar (loyihalar yechimi bo‘yicha dalillar va asosli argumentlarni taqdim qilish, eshitish va muammolar yechimini topish qobiliyatini rivojlantirish).

II-BO‘LIM.

MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

II. MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

“Blum kubigi” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni o‘zlashtirilishini yengillashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun “Ochiq” savollar tuzish va ularga javob topish mashqi vazifasini belgilaydi.

Metodni amalga oshirish tartibi:

1. Ushbu metodni ko‘llash uchun, oddiy kub kerak bo‘ladi. Kubning har bir tomonida ko‘yidagi so‘zlar yoziladi:
   - **Sanab bering, ta’rif bering (oddiy savol)**
   - **Nima uchun (sabab-oqibatni aniqlashtiruvchi savol)**
   - **Tushintirib bering (muammoni har tomonlama qarash savoli)**
   - **Taklif bering (amaliyot bilan bog‘liq savol)**
   - **Misol keltiring (ijodkorlikni rivojlantirovchi savol)**
   - **Fikr bering (tahlil kilish va baxolash savoli)**

2. O‘qituvchi mavzuni belgilab beradi.

3. O‘qituvchi kubikni stolga tashlaydi. Qaysi so‘z chiqsa, unga tegishli savolni beradi.

“KWHL” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborot tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha quyidagi jadvalda berilgan savollarga javob topish mashqi vazifasini belgilaydi.

Izoh. *KWHL:*
Know – nimalarni bilaman?
Want – nimani bilishni xohlayman?
How - qanday bilib olsam bo‘ladi?
Learn - nimani o‘rganib oldim?.

“KWHL” metodi	
1. Nimalarni bilaman: -	*2. Nimalarni bilishni xohlayman, nimalarni bilishim kerak:* -
3. Qanday qilib bilib va topib olaman: -	*4. Nimalarni bilib oldim:* -

“5W1H” metodi

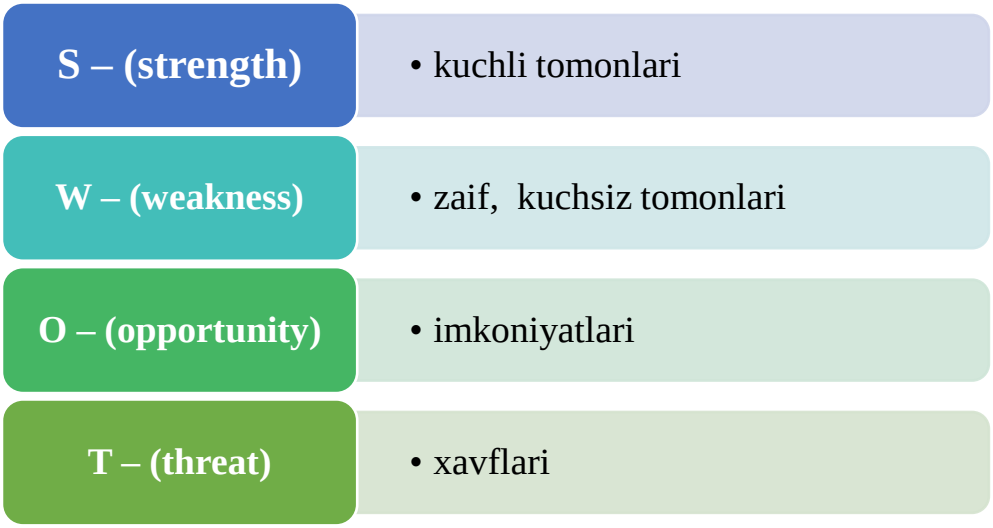
Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborot tizimini qabul qilish va bilimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha qo‘yidagi jadvalda berilgan oltita savollarga javob topish mashqi vazifasini belgilaydi.

What?	Nima? (ta’rifi, mazmuni, nima uchun ishlatiladi)	
Where?	Qayerda (joylashgan, qayerdan olish mukin)?	
What kind?	Qanday? (parametrlari, turlari mavjud)	
When?	Qachon? (ishlatiladi)	
Why?	Nima uchun? (ishlatiladi)	
How?	Qanday qilib? (yaratiladi, saqlanadi, to‘ldiriladi, tahrirlash mumkin)	

“SWOT-tahlil” metodi

Metodning maqsadi: mavjud nazariy bilimlar va amaliy tajribalarni tahlil qilish, taqqoslash orqali muammoni hal etish yo‘llarini topishga, bilimlarni

mustahkamlash, takrorlash, baholashga, mustaqil, tanqidiy fikrlashni, nostandart tafakkurni shakllantirishga xizmat qiladi.



“VEYER” metodi

Metodning maqsadi: Bu metod murakkab, ko‘ptarmoqli, mumkin qadar, muammoli xarakteridagi mavzularni o‘rganishga qaratilgan. Metodning mohiyati shundan iboratki, bunda mavzuning turli tarmoqlari bo‘yicha bir xil axborot beriladi va ayni paytda, ularning har biri alohida aspektlarda muhokama etiladi. Masalan, muammo ijobiy va salbiy tomonlari, afzallik, fazilat va kamchiliklari, foyda va zararlari bo‘yicha o‘rganiladi. Bu interfaol metod tanqidiy, tahliliy, aniq mantiqiy fikrlashni muvaffaqiyatli rivojlantirishga hamda o‘quvchilarning mustaqil g‘oyalari, fikrlarini yozma va og‘zaki shaklda tizimli bayon etish, himoya qilishga imkoniyat yaratadi. “Veyer” metodidan ma’ruza mashg‘ulotlarida individual va juftliklardagi ish shaklida, amaliy va seminar mashg‘ulotlarida kichik guruhlardagi ish shaklida mavzu yuzasidan bilimlarni mustahkamlash, tahlil qilish va taqqoslash maqsadida foydalanish mumkin.

Metodni amalga oshirish tartibi:

trener-o‘qituvchi ishtirokchilarni 5-6 kishidan iborat kichik guruhlarga ajratadi;

trening maqsadi, shartlari va tartibi bilan ishtirokchilarni tanishtirgach, har bir guruhga umumiy muammoni tahlil qilinishi zarur bo‘lgan qismlari tushirilgan tarqatma materiallarni tarqatadi;

har bir guruh o‘ziga berilgan muammoni atroflicha tahlil qilib, o‘z mulohazalarini tavsiya etilayotgan sxema bo‘yicha tarqatmaga yozma bayon qiladi;

navbatdagi bosqichda barcha guruhlar o‘z taqdimotlarini o‘tkazadilar. Shundan so‘ng, trener tomonidan tahlillar umumlashtiriladi, zaruriy axborotlr bilan to‘ldiriladi va mavzu yakunlanadi.

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

“Keys-stadi” metodi

«Keys-stadi» - inglizcha so‘z bo‘lib, («case» – aniq vaziyat, hodisa, «stady» – o‘rganmoq, tahlil qilmoq) aniq vaziyatlarni o‘rganish, tahlil qilish asosida o‘qitishni amalga oshirishga qaratilgan metod hisoblanadi. Mazkur metod dastlab 1921 yil Garvard universitetida amaliy vaziyatlardan iqtisodiy boshqaruv fanlarini o‘rganishda foydalanish tartibida qo‘llanilgan. Keysda ochiq axborotlardan yoki aniq voqea-hodisadan vaziyat sifatida tahlil uchun foydalanish mumkin.

“Keys metodi” ni amalga oshirish bosqichlari

Ish bosqichlari	Faoliyat shakli va mazmuni
1-bosqich: Keys va uning axborot ta’minoti bilan tanishtirish	✓ yakka tartibdagi audio-vizual ish; ✓ keys bilan tanishish(matnli, audio yoki media shaklda); ✓ axborotni umumlashtirish; ✓ axborot tahlili; ✓ muammolarni aniqlash
2-bosqich: Keysni aniqlashtirish va o‘quv topshirig‘ni belgilash	✓ individual va guruhda ishlash; ✓ muammolarni dolzarblik iyerarxiyasini aniqlash; ✓ asosiy muammoli vaziyatni belgilash
3-bosqich: Keysdagi asosiy muammoni tahlil etish orqali o‘quv topshirig‘ining yechimini izlash, hal etish yo‘llarini ishlab chiqish	✓ individual va guruhda ishlash; ✓ muqobil yechim yo‘llarini ishlab chiqish; ✓ har bir yechimning imkoniyatlari va to‘siqlarni tahlil qilish; ✓ muqobil yechimlarni tanlash
4-bosqich: Keys yechimini yechimini shakllantirish va asoslash, taqdimot.	✓ yakka va guruhda ishlash; ✓ muqobil variantlarni amalda qo‘llash imkoniyatlarini asoslash; ✓ ijodiy-loyiha taqdimotini tayyorlash; ✓ yakuniy xulosa va vaziyat yechimining amaliy aspektlarini yoritish

“Assesment” metodi

Metodning maqsadi: mazkur metod ta’lim oluvchilarning bilim darajasini baholash, nazorat qilish, o‘zlashtirish ko‘rsatkichi va amaliy ko‘nikmalarini tekshirishga yo‘naltirilgan. Mazkur texnika orqali ta’lim oluvchilarning bilish faoliyati turli yo‘nalishlar (test, amaliy ko‘nikmalar, muammoli vaziyatlar mashqi, qiyosiy tahlil, simptomlarni aniqlash) bo‘yicha tashhis qilinadi va baholanadi.

Metodni amalga oshirish tartibi:

“Assesment”lardan ma’ruza mashg‘ulotlarida talabalarning yoki qatnashchilarning mavjud bilim darajasini o‘rganishda, yangi ma’lumotlarni bayon qilishda, seminar, amaliy mashg‘ulotlarda esa mavzu yoki ma’lumotlarni o‘zlashtirish darajasini baholash, shuningdek, o‘z-o‘zini baholash maqsadida individual shaklda foydalanish tavsiya etiladi. Shuningdek, o‘qituvchining ijodiy yondashuvi hamda o‘quv maqsadlaridan kelib chiqib, assesmentga qo‘shimcha

topshiriqlarni kiritish mumkin.

Har bir katakdagi to‘g‘ri javob 5 ball yoki 1-5 balgacha baholanishi mumkin.

Test

Muammoli vaziyat

Tushuncha tahlili (simptom)

Amaliy vazifa

“Insert” metodi

Metodni amalga oshirish tartibi:

➢ o‘qituvchi mashg‘ulotga qadar mavzuning asosiy tushunchalari mazmuni yoritilgan matnni tarqatma yoki taqdimot ko‘rinishida tayyorlaydi;

➢ yangi mavzu mohiyatini yorituvchi matn ta’lim oluvchilarga tarqatiladi yoki taqdimot ko‘rinishida namoyish etiladi;

➢ ta’lim oluvchilar individual tarzda matn bilan tanishib chiqib, o‘z shaxsiy qarashlarini maxsus belgilar orqali ifodalaydilar. Matn bilan ishlashda talabalar yoki qatnashchilarga quyidagi maxsus belgilardan foydalanish tavsiya etiladi:

Belgilar	Matn
“V” – tanish ma’lumot.	
“?” – mazkur ma’lumotni tushunmadim, izoh kerak.	
“+” bu ma’lumot men uchun yangilik.	
“– ” bu fikr yoki mazkur ma’lumotga qarshiman?	

Belgilangan vaqt yakunlangach, ta’lim oluvchilar uchun notanish va tushunarsiz bo‘lgan ma’lumotlar o‘qituvchi tomonidan tahlil qilinib, izohlanadi, ularning mohiyati to‘liq yoritiladi. Savollarga javob beriladi va mashg‘ulot yakunlanadi.

III BO‘LIM.

NAZARIY MATERIALLAR

III. NAZARIY MATERIALLAR

1-ma’ruza. YENGIL VAZNLI KRIPTOGRAFIYA (YVK) (2 soat)

Reja:

1.1. Buyumlar Interneti.
1.2. Imkoniyati cheklangan muhit, qurilmalar va ularning xususiyatlari.
1.3. Ananaviy kriptografik algoritmlarni amalga oshirishdagi muammolar.

Tayanch iboralar: *Buyumlar Interneti, imkoniyati cheklangan, IoT, aqlli shahar, sensor, mikrokontroller, RAM, ROM, Arduino, yengil vaznli kriptografiya, quvvat.*

1.1. Buyumlar Interneti

Buyumlar Interneti (Internet of Things, IoT) o‘rnatilgan (embedded) razvedka, aloqa vositalari, sezish va ishga tushirish imkoniyatlariga ega milliardlab ob’ektlar IP (Internet Protocol) tarmoqlari orqali ulanadigan dunyo haqidagi tasavvurni qamrab oladi. Hozirgi Internet apparat ta’minotidan (kompyuterlar, optic tolalar va Ethernet kabellari) bozorga asoslangan (Facebook, Amazon) imkoniyatlarga tubdan o‘tishni boshdan kechirdi. Bu kuchli gorizontal dasturiy ta’minot imkoniyatlariga ega bo‘lgan bir-biri bilan uzviy bog‘liq bo‘lgan intranetlarning o‘zaro bog‘lanishi tufayli yuzaga keldi. IoT ochiq muhitlarni va o‘zaro ishlaydigan platformalarning integratsiyalashgan arxitekturasini talab qiladi. Aqlli ob’ektlar va kiber-fizik tizimlar - yoki shunchaki “buyumlar” - bu yangi IoT ob’ektlari: kundalik hayot ob’ektlari, mikro-kontrollerlar, optik va/yoki radio uzatgichlar, sensorlar, ishga tushiruvchi mexanizmlar va aloqa uchun mos protokollar steklari bo‘lib, ular hisoblash, ma’lumot almashinish, saqlash uchun cheklangan imkoniyatlarga ega. Ushbu ob’ektlar foydalanuvchilar tomonidan birga olib yurilishi yoki atrof-muhitga joylashtirilishi mumkin. Ular odatda juda cheklangan, chegaralangan xotira va mavjud energiya zaxiralariga ega va ularga arzon narxda bo‘lishi kabi qat’iy talablar qo‘yiladi. Ma’lumotlarni saqlash, qayta ishlash va tahlil qilish IoTning ishlov berilmagan malumotlarini boyitish va ularni foydali ma’lumotlarga aylantirish uchun zarur bo‘lgan asosiy talablardir. “Edge Computing” paradigmasiga ko‘ra, foydalanish tarmoqlarining chetki qismida hisoblash resurslarini joriy qilish IoT ssenariylari uchun muhim bo‘lgan bir qancha afzalliklarni keltirishi mumkin: past kechikish, real vaqtda imkoniyatlar va kontekstdan xabardorlik. Chetki tugunlar (serverlar yoki chekkadagi mikro ma’lumotlar markazlari) ulangan qurilmalar, ob’ektlar va ilovalardan keladigan ma’lumotlar oqimlari uchun interfeys vazifasini bajarishi mumkin. Saqlangan Katta ma’lumotlar (Big Data) keyinchalik ulangan ob’ektlar tomonidan yaratilgan dastlabki ishlov berilmagan ma’lumotlarni foydali ma’lumotlarga aylantirib, mashinali va chuqur o‘rganish kabi yangi mexanizmlar bilan qayta ishlanishi mumkin. Keyin foydali ma’lumotlar tegishli qurilmalar va manfaatdor foydalanuvchilarga tarqatiladi yoki keyingi ishlov berish va foydalanish uchun saqlanadi.

IoT ilovalari

IoT hayotimizning barcha jabhalariga ta’sir qiladi. IoTni qo‘llab-quvvatlaydigan ilovalar juda ko‘p ssenariylarda topiladi, jumladan: uy va binolarni avtomatlashtirish, aqlli shaharlar, aqlli tarmoqlar, sanoat 4.0 va aqlli qishloq xo‘jaligi. Ushbu sohalarning har birida umumiy (IPga yo‘naltirilgan) aloqa protokoli stekidan foydalanish innovatsion ilovalarni yaratishga imkon beradi. Ushbu bo‘limda ushbu sohalarning har birida mumkin bo‘lgan ilovalarning qisqacha ko‘rinishi taqdim etiladi.

Uy va binolarni avtomatlashtirish

Aqlli uy bozori o‘sib borayotgan investitsiyalarga qarab rivojlanishda davom etar ekan, bu o‘z navbatida har biri ma’lum bir auditoriya uchun mo‘ljallangan uyni avtomatlashtirish dasturlari paydo bo‘lishiga olib kelmoqda. Natijada bir nechta uzilgan vertikal bozor segmentlari yaratildi. Borgan sari kengayib borayotgan asosiy ilovalarning odatiy misollari uy xavfsizligi, energiya samaradorligi va energiyani tejash bilan bog‘liq. Yorug‘lik va xonani boshqarish sohasidagi innovatsiyalardan kelib chiqqan holda, IoT uyni avtomatlashtirish uchun cheksiz ilovalarni ishlab chiqishga yordam beradi. Masalan, IoT kontekstida o‘sishga mo‘ljallangan uyni avtomatlashtirish sohasining xususiy misoli sog‘liqni saqlash sohasida, ya’ni jismoniy jihatdan kamroq harakat qiluvchilar (keksalar), nogironlar yoki surunkali kasalliklarga chalinganlar uchun (masalan, sog‘liqni saqlashni masofadan kuzatish va havo sifatini monitoring qilish) ishlab chiqilmoqda. Umuman olganda, binolarni avtomatlashtirish yechimlari birlasha boshlab, ayni paytda hashamatli, xavfsizlik va qulaylikdagi joriy ilovalardan kengroq ilovalar va ulangan echimlarga o‘tilmoqda; bu esa bozor imkoniyatlarini yaratadi. Bugungi aqlli uy echimlari fragmentlarga ajratilgan bo‘lsada, IoT tijorat uylar va binolarni avtomatlashtirish echimlari o‘rtasida o‘zaro muvofiqlikning yangi darajasiga olib kelishi kutilmoqda.

Aqlli shaharlar

Shaharlar murakkab ekotizimlar bo‘lib, bu yerda hayot sifati muhim ahamiyatga ega. Bunday shahar muhitida odamlar, kompaniyalar va davlat organlari sog‘liqni saqlash, ommaviy axborot vositalari, energiya va atrof-muhit, xavfsizlik va davlat xizmatlari kabi sohalarda o‘ziga xos ehtiyoj va talablarni boshdan kechirmoqda. Shahar tobora ko‘proq yagona “organizm” sifatida qabul qilinmoqda, uni fuqarolarga aniq ma’lumot bilan ta’minlash uchun samarali nazorat qilish kerak bo‘ladi. IoT texnologiyalari shahar holati to‘g‘risidagi ma’lumotlarni to‘plash va ularni fuqarolarga tarqatish uchun muhim hisoblanadi. Shu nuqtai nazardan, IoTga asoslangan ilg‘or xizmatlarga talabni shakllantirishda shaharlar juda muhim yuklama hisoblanadi.

Aqlli energetik tarmoqlar

Aqlli energetik tarmoq - bu aqlli hisoblagichlar, aqlli qurilmalar, qayta tiklanadigan energiya manbalari va energiya tejaydigan resurslarni o‘z ichiga olgan turli operatsion tizimlariga ega elektr tarmog‘idir. Elektr uzatish liniyalari aloqalari (Power line communications, PLC) ma’lumotlarni tashish uchun mavjud elektr kabellaridan foydalanish bilan bog‘liq va uzoq vaqt davomida tatqiq etilgan. Elektr ta’minoti korxonalari ushbu texnologiyadan ko‘p yillar davomida mavjud elektr tarmog‘i bo‘yicha ma’lumotlarni jo‘natish yoki qabul qilish (cheklangan miqdorda)

uchun foydalanmoqda. PLC asosan tarqalish muhiti turi bilan cheklangan bo‘lsada, u tarqatish tarmog‘idagi mavjud simlardan foydalanishi mumkin. Evropa Ittifoqi standartlari va qonunlariga ko‘ra, elektr ta’minoti kompaniyalari 3-148 kHz chastota diapazonida past bit tezligi (50 Kbit / s dan past ma’lumotlar tezligi bilan) uchun PLCdan foydalanishi mumkin. Ushbu texnologiya aqlli o‘lchash xizmatlari va energiya iste’moli hisoboti kabi ko‘plab amaliy sohalarda odamlar va buyumlar o‘rtasida yangi imkoniyatlar va o‘zaro munosabatlarning yangi shakllarini yaratadi. Bu PLC ni aqlli shahar va aqlli tarmoq ssenariylari kabi nisbatan keng hududlarga tarqalgan yirik tizimlarda sezish, boshqarish va avtomatlashtirishda foydalanish imkonini beradi. PLCdan tashqari, IoT kabi aqlli avtomatlashtirish jarayonlarini yaxshilaydigan faol texnologiyalarni ham qo‘llash mumkin. Masalan, PLC texnologiyasini sanoat ssenariylarida (masalan, avtomatlashtirish va ishlab chiqarish kompaniyalarida masofadan boshqarish) qabul qilinishi “Sanoat IoT” (Industrial IoT) ga yo‘l ochadi. PLC texnologiyasining tarmoqdagi o‘zgarishlardan (ta’mirlash va takomillashtirish, jismoniy o‘chirish va uzatish funksiyasi nuqtai nazaridan) signal uzatishdagi nosozliklarni kamaytirish qobiliyati tufayli bir nechta ilovalarda qo‘llanilgan.

Shunga qaramay, ma’lumki, elektr uzatish liniyalari ma’lumotlarni uzatish uchun ideal kanallardan (joylashuv, vaqt, chastota diapazoni va liniyaga ulangan uskunalar turidagi ichki o‘zgarishlar tufayli) ancha farq qiladi. Natijada, aloqa mustahkamligini oshirish uchun IoT va PLC paradigmalarini birgalikda qabul qilishga harakatlar ortmoqda. Bu keng tarqalgan hisoblash imkoniyatlariga ega bo‘lgan kichik, resurslari cheklangan qurilmalardan (masalan, IoT) va Internet standart echimlaridan (IETF, ETSI va W3C kabi Internet standartlashtirish tashkilotlari tomonidan taklif qilinganidek) foydalanish taklifiga olib keldi. Bunday tizimlar kelajakdagi aqlli tarmoqlarni amalga oshirish uchun asosiy komponentlar bo‘lishi ham mumkin.

Sanoatlashgan IoT

Sanoatlashgan IoT (Industrial Internet of Things, IIoT) IoTni ishlab chiqarish, logistika, neft va gaz, transport, energetika/kommunal xizmatlar, tog‘-kon sanoati va metallar, aviatsiya va boshqa sohalarda qo‘llaniladigan sifatida tavsiflaydi. Bu tarmoqlar G20 davlatlari orasida yalpi ichki mahsulotning asosiy qismini tashkil qiladi. IIoT hali ham dastlabki bosqichda, xuddi 1990-yillarning oxirida Internet bo‘lgan joyga o‘xshaydi. So‘nggi yigirma yil ichida iste’molchi Interneti evolyutsiyasi ba’zi muhim saboqlarni taqdim etgan bo‘lsada, uning noyob ko‘lami va talablarini hisobga olgan holda, ushbu o‘rganishning IIoT uchun qanchalik qo‘llanilishi aniq emas. Masalan, ishlab chiqarish, energiya, transport va sog‘liqni saqlash sohalarida real vaqt rejimidagi javoblar ko‘pincha muhim ahamiyatga ega: bugungi Internet uchun real vaqt odatda bir necha soniyani anglatadi, sanoat mashinalari uchun real vaqt millisekunddan ham kichik shkalalarni o‘z ichiga oladi. Yana bir muhim omil - bu ishonchlilik. Hozirgi Internet “eng yaxshi yetkazib berish” yondashuvini o‘zida mujassam etgan bo‘lib, u elektron tijorat yoki odamlarning o‘zaro munosabatlari uchun maqbul samaradorlikni ta’minlaydi. Biroq, elektr tarmog‘i, havo harakatini boshqarish tizimi yoki avtomatlashtirilgan zavodning bir xil vaqt davomida ishlamay qolishi jiddiyroq oqibatlarga olib keladi.

Cisco, GE va Huawei kabi yirik kompaniyalarning say-harakatlariga va Germaniyadagi Industrie 4.0 kabi hukumat tashabbuslariga katta e'tibor berilmoqda. Masalan:

• GE mijozlarga IIoT imkoniyatlari va xizmatlari orqali aktivlar unumdorligi va biznes operatsiyalarini yaxshilashga yordam berish orqali 2014-yilda 1 milliard dollardan ortiq qo‘shimcha daromad olganini e'lon qildi.

• Germaniya hukumati "Industrie 4.0" nomli ko‘p yillik strategik tashabbusga homiylik qilmoqda, u nemis sanoat sektoriga raqamli texnologiyalarni qo‘llash bo‘yicha keng qamrovli qarash va harakatlar rejasini yaratish uchun davlat va xususiy sektorlar hamda akademik doiralar yetakchilarini birlashtiradi.

• Boshqa Evropa mamlakatlarida IIoT markaziy o‘rinni egallagan sanoat transformatsiyasi bo‘yicha o‘zlarining loyihalari mavjud, masalan, Smart Factory (Gollandiya), Industry 4.0 (Italiya), Industry of Future (Fransiya) va boshqalar.

• Xitoy ham yaqinda raqamli texnologiyalar va sanoatlashtirishning ichki integratsiyasini rag‘batlantirish maqsadida "Made in China 2025" strategiyasini ishga tushirdi.

IIoT jadallashib borayotganligi sababli, duch keladigan eng katta qiyinchiliklardan biri bu turli "tillarda" gaplashishi mumkin bo‘lgan aqlli qurilmalar o‘rtasida ma'lumot almashishning mumkin emasligidir. Ushbu aloqa bo‘shlig‘i zavod darajasida ishlatiladigan bir nechta protokollardan kelib chiqadi. Shunday qilib, ma'lumot to‘plash uchun sensorni mashinaga o‘rnatishingiz mumkin bo‘lsada, bu ma'lumotni tarmoq bo‘ylab uzatish va oxir-oqibat boshqa tizimlar bilan "suhbatlashish" biroz qiyinroq. Shuning uchun standartlashtirish IIoT ning asosiy jihati hisoblanadi.

IIoTning potentsial foydasi juda katta. Operatsion samaradorlik uning asosiy diqqatga sazovor joylaridan biri bo‘lib, erta qabul qiluvchilar ushbu imtiyozlarga e'tibor qaratishadi. Avtomatlashtirish va yanada moslashuvchan ishlab chiqarish texnikasini joriy qilish orqali, masalan, ishlab chiqaruvchilar o‘z mahsuldorligini 30% ga oshirishlari mumkin. Shu nuqtai nazardan, uchta IIoT qobiliyatini o‘zlashtirish kerak:

• *sensorga asoslangan hisoblash:* sezilgan ma'lumotlarni operatorlar va tizimlar harakat qilishi mumkin bo‘lgan tushunchalarga aylantirish;

• *sanoat tahlili:* datchiklar va boshqa manbalardan olingan ma'lumotlarni amaldagi tushunchalarga aylantirish;

• *aqlli mashina ilovalari:* sensorli qurilmalar va aqlli komponentlarni mashinalarga birlashtirish.

Aqlli qishloq xo‘jaligi

Zamonaviy qishloq xo‘jaligi dunyoning turli mintaqalarida barqaror kelajakni qurishga intilayotgani sababli ulkan muammolarga duch kelmoqda. Bunday muammolarga misollar orasida aholining ko‘payishi, urbanizatsiya, tobora yomonlashib borayotgan atrof-muhit, hayvonlar oqsillarini iste'mol qilish tendentsiyasi, aholining qarishi va migratsiya natijasida oziq-ovqat imtiyozlarining o‘zgarishi va albatta, iqlim o‘zgarishi kiradi. Ilm-fan yutuqlari, tadqiqot va tajriba-konstruktorlik faoliyati natijalaridan olingan ishlab chiqarish jarayonlari, texnologiyalar va vositalarni o‘zlashtirish bilan tavsiflangan zamonaviy qishloq

xo‘jaligini rivojlantirish kerak bo‘ladi.

Aqlli qishloq xo‘jaligi raqamli rivojlanish uchun eng katta imkoniyatlarga ega, ammo raqamli yechimlarning hozirgi kunga qadar eng past kirib borgan sohasidir. Kelgusi bir necha o‘n yilliklarda qishloq xo‘jaligi sanoati har qachongidan ham muhimroq bo‘ladi. Bu atrof-muhit va yerdagi sensorlardan, ob-havoni kuzatish uchun ilovalardan, o‘g‘itlar va kimyoviy moddalarni (shunday qilib, tabiiy resurslarning isrofgarchiligini kamaytiradi) yanada aniqroq qo‘llashni avtomatlashtirishdan va texnik xizmat ko‘rsatishni rejalashtirish strategiyalarini qabul qilishdan katta foyda keltirishi mumkin.

Dronlar va sensorli tarmoqlar (ma’lumotlarni yig‘ish uchun) va bulutli platformalar (to‘plangan ma’lumotlarni boshqarish uchun) kabi yangi texnologiyalarni qo‘llash tufayli aqlli qishloq xo‘jaligi allaqachon keng tarqalmoqda. Aqlli qishloq xo‘jaligida qo‘llaniladigan texnologiyalar majmuasi fermerlar, paxtakorlar va sohadagi boshqa manfaatdor tomonlar tomonidan boshqariladigan faoliyat kabi murakkabdir. Keng ko‘lamli ilovalar mavjud: avtoparkni boshqarish, chorvachilik monitoringi, baliq etishtirish, o‘rmon parvarishi, yopiq shahar dehqonchiligi va boshqalar. Ishtirok etilgan barcha texnologiyalar IoT kontseptsiyasi atrofida aylanadi va qarorlarni qo‘llab-quvvatlash tizimlari orqali fermerlarni qaror qabul qilish jarayonida qo‘llab-quvvatlashga qaratilgan. Ular real vaqt rejimidagi ma’lumotlarni ilgari mumkin bo‘lmagan miqdoriy darajada bo‘lishini o‘z ichiga oladi. Bu kamroq isrofgarchilikka va samaradorlikni oshirishga olib keladigan yaxshiroq qarorlar qabul qilish imkonini beradi.

Aloqa texnologiyalari aqlli qishloq xo‘jaligi ilovalarining asosiy tarkibiy qismidir. Xususan, simsiz aloqa texnologiyalari simsiz ulanishning sezilarli darajada qisqarishi va soddalashtirilganligi tufayli muhimligi ortib bormoqda. Har xil simsiz aloqa standartlari o‘rnatildi. Uzatish diapazoniga qarab ularni ikkita asosiy toifaga guruhlash mumkin:

- *Qisqa masofali aloqa:* quyidagilar uchun standartlarni o‘z ichiga oladi:
  – Wi-Fi uchun ishlatiladigan simsiz LAN, ya’ni IEEE 802.11;
  – IEEE 802.15.1 (Bluetooth) (IEEE, 2002) va IEEE 802.15.4 (ZigBee/6LoWPAN) (IEEE, 2003) kabi o‘lchash va avtomatlashtirish ilovalari uchun kengroq qo‘llaniladigan simsiz PAN;

Ushbu standartlarning barchasi odatda 2,400–2,4835 GGts diapazonida ishlaydigan asbob-uskunalar, ilmiy va tibbiy (instrumentation, scientific and medical, ISM) radio diapazonlaridan foydalanadi.

- *Uzoq masofali aloqa:* 868–870 MGts diapazonida LoRA kabi tobora muhim bo‘lgan IoT aloqa texnologiyalarini o‘z ichiga oladi. Bu uzoqroq uzatish diapazonlari uchun ma’lumotlarni uzatish tezligini (yuzlab kbit/s gacha) hosil qiladi.

Maxsus qo‘llanilishiga ko‘ra aloqa texnologiyalari ham tasniflanishi mumkin:

- atrof-muhit monitoringi (ob-havo monitoringi va geo-ma’lumotli atrof-muhit monitoringi);
- texnologiyalashgan qishloq xo‘jaligi (precision agriculture);
- mashina va jarayonni boshqarish (M2M aloqa);
- ob’ektni avtomatlashtirish;

- kuzatuv tizimlari.

1.2. Imkoniyati cheklangan muhit, qurilmalar va ularning xususiyatlari

IoT hozirgi kunda milliardlab qurilmalarni o‘z ichiga olgan butun dunyo bo‘ylab tarmoq bo‘lishi kutilmoqda. Keng tarqalgan bo‘lib qo‘llaniladigan ushbu ulkan miqdordagi qurilmalar dasturiy ta’minot va xususan, apparat jihatidan bir xil emasligi bilan tavsiflanadi.

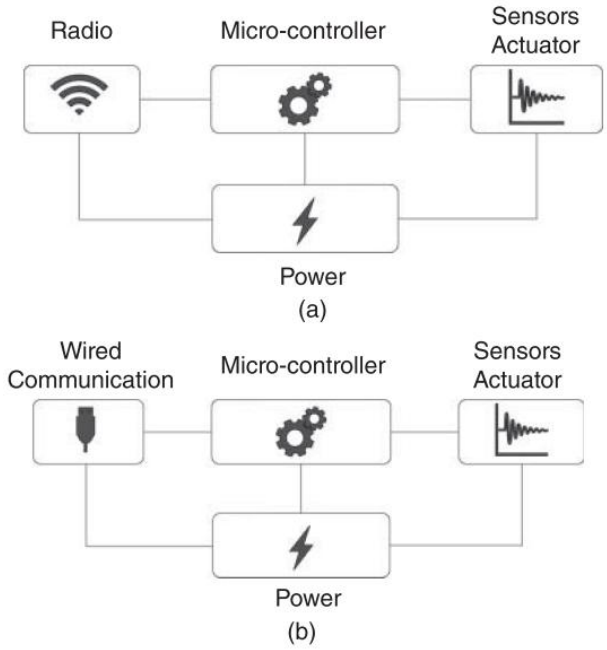
Uskuna platformalarining umumiy ta’rifini berish uchun 1.1-rasmda aqlli ob’ektdagi asosiy apparat komponentlarining yuqori darajadagi ko‘rinishi ko‘rsatilgan. Undagi asosiy modullar:

• *Aloqa moduli:* Bu aqlli ob’ektga aloqa o‘rnatish imkoniyatlarini beradi. Bu odatda antena yoki simli ulanishga ega radio qabul qiluvchi bo‘lishi mumkin.

• *Mikrokontroller:* Bu aqlli ob’ektga o‘z harakatini beradi. Bu aqlli ob’ektning dasturiy ta’minotini boshqaradigan kichik mikroprotsessor.

• *Sensorlar yoki bajaruvchi mexanizmlar:* Bular aqlli ob’ektga fizik dunyoni his qilish va o‘zaro aloqada bo‘lish usulini beradi.

• *Quvvat manbai:* Aqlli ob’ektda elektr zanjiri mavjudligi bois, ushbu tashkil etuvchi zarur. Eng keng tarqalgan quvvat manbai batareyadir, lekin boshqa misollar ham mavjud, masalan, jismoniy kuch qo‘llanilganda quvvatni ta’minlaydigan piezoelektrik quvvat manbalari yoki yorug‘lik paydo bo‘lganda quvvatni ta’minlaydigan kichik quyosh batareyalari.



1.1-rasm. (a) radio tarmoq interfeysi va (b) simli aloqa interfeysiga ega aqlli ob’ekt apparati

Mikrokontrollerlar ikki xil xotiraga ega: faqat o‘qish uchun mo‘ljallangan xotira (Read-only memory, ROM) va tasodifiy foydalanish xotirasi (Random access memory, RAM). ROM qurilmaning harakatini ifodalaydigan dastur kodini saqlash uchun ishlatiladi va RAM dasturiy ta’minot o‘z vazifasini bajarishi kerak bo‘lgan vaqtinchalik ma’lumotlar uchun ishlatiladi. Masalan, vaqtinchalik ma’lumotlarga dastur o‘zgaruvchilari uchun saqlash va radio trafigini boshqarish uchun bufer xotira kiradi.

Cheklangan qurilmalar uchun ROM tarkibi odatda ishlab chiqarilganda qurilmaga yoziladi va tarqatilgandan keyin o‘zgartirilmaydi. Zamonaviy mikrokontrollerlar ROMni qayta yozish mexanizmini ta’minlaydi, bu qurilmalar o‘rnatilgandan so‘ng dasturiy ta’minotni yangilash uchun foydali hisoblanadi.

Mikrokontrollerlar dastur kodini va vaqtinchalik o‘zgaruvchilarni saqlash uchun xotiradan tashqari, aloqa qurilmalari, sensorlar va aktuatorlar kabi tashqi qurilmalar bilan o‘zaro ta’sir qilish uchun taymerlar va mexanizmlar to‘plamini o‘z ichiga oladi. Taymerlar mikrokontrollerda ishlaydigan dasturiy ta’minot tomonidan erkin ishlatilishi mumkin. Tashqi qurilmalar fizik ravishda uning pinlariga ulangan. Dasturiy ta’minot mikrokontroller tomonidan taqdim etilgan mexanizmlar yordamida ketma-ket port yoki ketma-ket avtobus ko‘rinishida qurilmalar bilan aloqa qiladi. Aksariyat mikrokontrollerlar ketma-ket portlar bilan aloqa qilish uchun universal sinxron/ asinxron qabul qiluvchi/ uzatuvchi (Universal synchronous/ asynchronous receiver/ transmitter, USART) deb ataladigan narsalarni taqdim etadi. Ba’zi USARTlar sensorlar va bajaruvchi mexanizmlar bilan aloqa qilish uchun ketma-ket periferik interfeys (Serial peripheral interface, SPI) shinasi sifatida ishlash uchun sozlanishi mumkin.

Aqlli ob’ekt elektron mexanizm tomonidan boshqariladi va bu mexanizm quvvatga muhtoj. Shuning uchun har bir aqlli ob’ekt quvvat manbaiga muhtoj (ba’zi quvvat manbalari 1.1-jadvalda keltirilgan). Bugungi kunda eng keng tarqalgan quvvat manbai batareyadir, lekin quyosh batareyalari, piezoelektrik, radio uzatiladigan energiya va quvvatni to‘plashning boshqa shakllari kabi quvvat uchun bir nechta boshqa imkoniyatlar mavjud. Hozirgi vaqtda litiyum batareyalar eng keng tarqalgan. Kam quvvatli uskuna va energiyani boshqarish bo‘yicha tegishli dasturiy ta’minot bilan aqlli ob’ekt standart litiyum batareyalarda bir necha yil xizmat qilishi mumkin. Inson tomonidan boshqariladigan mobil telefonlar va noutbuklardan farqli o‘laroq, aksariyat aqlli ob’ektlar inson nazoratisiz yoki inson qarovisiz ishlashga mo‘ljallangan. Bundan tashqari, ko‘plab aqlli ob’ektlar erishish qiyin bo‘lgan joylarda joylashgan va ko‘plari boshqa ob’ektlarga o‘rnatilgan. Shuning uchun ko‘p hollarda ularning batareyalarini qayta zaryadlash imkonsiz.

1.1-jadval

Aqlli ob’ektlar uchun quvvat manbalari, maksimal tok miqdori (typical maximum current) va ular saqlashi mumkin bo‘lgan zaryad (typical charge) miqdori

Power source	Typical maximum current (mA)	Typical charge (mAh)
CR2032 button cell	20	200
AA alkaline battery	20	3000
Solar cell	40	Limitless
RF power	25	Limitless

Imkoniyati cheklangan qurilmalar sinflari

Internetga ulangan qurilmalarning juda xilma-xilligiga qaramay, cheklangan qurilmalarning turli sinflari uchun umumiy terminologiyaga ega bo‘lish mutlaqo maqsadga muvofiq. Shu sababli, RFC7228 IoT aqlli ob’ektlari va cheklangan qurilmalarning asosiy sinflari va xususiyatlari uchun ta’rif bergan (1.2-jadval).

1.2-jadval

RFC7228da keltirilgan imkoniyati cheklangan qurilmalar sinflari

Name	Data size (e.g., RAM)	Code size (e.g., Flash)
Class 0 (C0)	≪10 KiB	≪100 KiB
Class 1 (C1)	~ 10 KiB	~ 100 KiB
Class 2 (C2)	~ 50 KiB	~ 250 KiB

Bu xususiyatlar imkoniyati chegaralangan qurilmalar uchun sotiladigan chiplar va dizayn yadrolarining ajralib turadigan klasterlariga mos keladi. Bu sinflarning chegaralari vaqt o‘tishi bilan siljishi kuzatiladi; Mur qonuni o‘rnatilgan makonda shaxsiy hisoblash qurilmalariga qaraganda kamroq samarali bo‘ladi, shuning uchun tranzistorlar soni va zichligi oshishi natijasida olingan daromadlar hisoblash quvvatining doimiy o‘sishiga qaraganda xarajat va quvvat talablarini kamaytirishga ko‘proq investitsiya qilinadi.

Batafsilroq, sinflar quyidagicha:

0-sinf (Class 0) qurilmalari imkoniyati juda cheklangan sensorga o‘xshash kichik elementdir. Ularning xotirasi va qayta ishlash imkoniyatlari shu qadar cheklanganki, ular Internet bilan xavfsiz tarzda to‘g‘ridan-to‘g‘ri bog‘lanish uchun zarur bo‘lgan resurslarga ega bo‘lmaydilar. Ushbu qurilmalar proksi-server, shlyuz yoki server vazifasini bajaradigan kattaroq qurilmalar yordamida Internet aloqalarida ishtirok etadi. 0-sinf qurilmalarini odatda an’anaviy ma’noda himoya qilish yoki har tomonlama boshqarish mumkin emas. Ular, ehtimol, juda kichik ma’lumotlar to‘plami bilan oldindan sozlanadi (va kamdan-kam hollarda qayta sozlanishi qilinadi). Boshqaruv maqsadlarida ular tirik qolish (keep-alive) signallariga javob berishlari va yoqish/o‘chirish yoki asosiy ishlash holati ko‘rsatkichlarini yuborishlari mumkin.

1-sinf (Class 1) qurilmalari kod sohasida va qayta ishlash imkoniyatlarida ancha cheklangan, shuning uchun ular HTTP, TLS (Transport Layer Security) va tegishli xavfsizlik protokollari va XMLga asoslangan ma’lumotlar taqdimoti kabi to‘liq protokollar stekidan foydalanadigan boshqa Internet tugunlari bilan osongina aloqa o‘rnata olmaydi. Ular cheklangan tugunlar uchun maxsus mo‘ljallangan protokollar stekidan foydalanishlari mumkin (masalan, UDP orqali CoAP) va shlyuz tugunlari yordamisiz mazmunli suhbatlarda qatnashishlari mumkin. Ular katta tarmoqda talab qilinadigan xavfsizlik funksiyalarini qo‘llab-quvvatlashi mumkin. Shuning uchun, ular IP tarmog‘iga to‘liq rivojlangan tugunlar sifatida birlashtirilishi mumkin, ammo ular holat xotirasi, kod maydoni va protokol va ilovalardan foydalanish uchun ko‘pincha quvvat sarfiga e’tibor qaratishlari kerak.

2-sinf (Class 2) qurilmalari kamroq cheklangan va asosan noutbuklar yoki

serverlarda ishlatiladigan protokollar steklarining ko‘pini qo‘llab-quvvatlashga qodir. Ular yengil va energiya tejovchi protokollardan va kamroq tarmoqning o‘tkazish qobiliyatidan foydalanishlari mumkin. Tarmoq uchun kamroq resurslardan foydalanish natijasida ilovalar uchun ko‘proq resurslar qoladi. Shunday qilib, 2-sinf qurilmalarida ko‘proq cheklangan qurilmalar uchun belgilangan protokol steklaridan foydalanish ishlab chiqish xarajatlarini kamaytirishi va o‘zaro muvofiqlikni oshirishi mumkin.

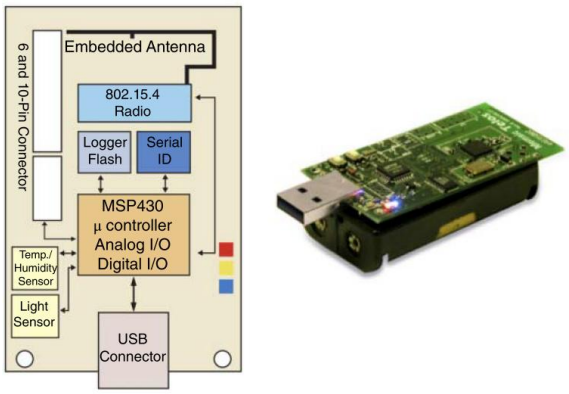
Quyida hozirda bozorda mavjud bo‘lgan ba’zi asosiy apparat platformalari bilan tanishiladi.

TelosB

TelosB - Memsic Technology kompaniyasining mahsuloti. U Sentilla kompaniyasining Tmote Sky qurilmasi bilan bir xil dizaynga ega. U MSP430 (MSP430F1611) mikrokontrolleri va CC2420 radio chipidan iborat. Ushbu qurilmaning mikrokontrolleri 415 MGts chastotada ishlaydi va 10 kB ichki operativ xotira va 48 kB dasturlashtiriladigan flesh xotiraga ega.

TelosB Berkli, Kaliforniya universiteti tomonidan ishlab chiqilgan. Bu avvalgi qurilma tajribasiga asoslangan yangi apparat loyihasi edi. U eksperiment o‘tkazishga imkon beradigan uchta asosiy maqsad bilan ishlab chiqilgan: minimal quvvat sarfi, foydalanish qulayligi va dasturiy ta'minot va apparatning mustahkamligini oshirish. MSP430ning Telosda qo‘llanilishi unga oldingi qurilma platformalarining deyarli o‘ndan bir quvvatini sarflash imkonini berdi.

1.2-rasmda qurilmaning sxematik ko‘rinishi va komponentlarning o‘zaro bog‘lanishi ko‘rsatilgan. 1.3-jadvalda modullar va ularga tegishli tavsiflar bilan batafsil apparat profili berilgan. Telos Bni 0-sinf cheklangan qurilma sifatida tasniflash mumkin.



1.2-rasm. TelosB qurilmasi platformasining apparat sxemasi va qurilma tasviri

1.3-jadval

MemSic TelosB qurilmasining tavsifi

Name	Description
MCU	TI MSP430F1611
RAM	10 kB
ROM	48 kB
Serial communication	UART
Main module current draw	1.8 mA (active mode)
	5.1 μA (sleep mode)
IEEE 802.15.4 compliant	
RF transceiver	2400–2483.5 MHz
RF current draw	23 mA (receive mode)
	21 μA (idle mode)
	1 μA (sleep mode)
Battery	2 × AA batteries
Sensors	Visible light sensor
	Humidity sensor
	Temperature sensor

Zolertia Z1

Zolertia Z1 simsiz sensor tarmoqlari va turli xil IoT ilovalariga mo‘ljallangan umumiy maqsadli ishlab chiqish platasidir. U ikkita bortdagi raqamli sensorlar (akselerometer va harorat sensori) bilan jihozlangan va sensorlar va bajaruvchi mexanizmlar kabi ulangan qurilmalarni osongina kengaytirish uchun Phidget Sensors ulagichlaridan foydalanadi.

1.4-jadvalda Z1 ning sxematik ko‘rinishi va komponentlarning o‘zaro ta’siri va ularning ulagichlari bilan mavjud sensorlarning qisqacha mazmuni keltirilgan. Telos B singari, Zolertia Z1 0-sinf cheklangan qurilma sifatida tasniflanishi mumkin.

1.4-jadval

Zolertia Z1 plaformasining qurilma tavsifi

Name	Description
MCU	TI MSP430F2617
RAM	8 kB
ROM	92 kB
Digital communication	I2C, SPI and UART
Main module current draw	0.5 mA (active mode)
	0.5 μA (standby mode)
IEEE 802.15.4 compliant	
RF transceiver	CC2420 2.4 GHz
RF current draw	18.8 mA (receive mode)
	426 μA (idle mode)
	20 μA (sleep mode)
Battery	2 × AA or AAA cells
	1 × CR2032 coin cell
Sensors	Low-power digital temperature sensor 3-axis, ±2/4/8/16*g* digital accelerometer, 3 V and 5 V Phidget Sensors connectors

OpenMote

OpenMote apparati uchta platadan iborat: OpenMoteCC2538, OpenBase va OpenBattery. OpenMote-CC2538 qurilmaning o‘zi bo‘lib, mikrokontroller va radio uzatgichni, shuningdek, LED va tugmalar kabi boshqa tashqi qurilmalarni o‘z ichiga oladi. OpenBase - bu kompyuter bilan UART yoki USB interfeysi yoki Internet bilan Ethernet porti orqali dasturlash va debaggerlash imkonini beruvchi plata. OpenBattery - bu OpenMote-CC2538 ning barcha quyi tizimlarini energiya bilan ta’minlash orqali avtonom ishlashga imkon beruvchi plata bo‘lib, uni turli sensorlar bilan ulash imkonini beradi.

OpenMote-CC2538 quyidagi uskunani o‘z ichiga oladi:

• CC2538: Bu 32-bitli Cortex-M3 mikrokontrolleri va CC2520ga o‘xshash radio qabul qiluvchiga ega Texas Instruments kompaniyasining chip (System on a chip, SoC) ustidagi tizim. Mikrokontroller 32 MGts gacha ishlaydi va 32 kB RAM va 512 kB flesh-xotira va odatdagi tashqi qurilmalarni (GPIO, ADC, taymerlar va boshqalar) o‘z ichiga oladi. Radio 2,4 gigagersli diapazonda ishlaydi va IEEE 802.15.4-2006 standartiga to‘liq mos keladi.

• TPS62730: Bu Texas Instruments kompaniyasining ikki ish rejimiga ega bo‘lgan kamayuvchi (step-down) DC/DC konvertori: tartibga solinadigan va aylanib o‘tish. Bypass rejimida TPS62730 to‘g‘ridan-to‘g‘ri batareyadan kirish kuchlanishini (odatda 3 V) butun tizimga ulaydi. Tartibga solingan rejimda TPS62730 kirish kuchlanishini 2,1 V ga tushiradi. Ushbu arxitekturaning foydasi tizim samaradorligi nuqtai nazaridan bo‘lib, u past va yuqori yuk sharoitida yaxshilanadi; ya’ni tizim uxlayotganda yoki radio uzatish yoki qabul qilishida.

• ABM8G: Bu Abracon korporatsiyasining 32 MGts chastotali kristali bo‘lib, mikrokontroller va radio qabul qiluvchini aniqlash (clock) uchun ishlatiladi. −20◦C dan +70◦C gacha bo‘lgan haroratda 30 ppm (milliondagi qismlar) xatolik bilan ishlaydi.

• ABS07: Bu Abracon korporatsiyasining 32,768 kHz kristalli bo‘lib, mikrokontrollerning real vaqt soatini hisoblash uchun ishlatiladi. −40◦C dan +85◦C gacha haroratda 10 ppm xatolik bilan ishlaydi.

• LEDlar: Rohm Semiconductordan to‘rtta LED (qizil, yashil, sariq va to‘q sariq) mavjud bo‘lib, ular debaggerlash maqsadida ishlatiladi.

• Tugmalar: Omrondan ikkita tugma mavjud. Ulardan biri platani qayta o‘rnatish uchun ishlatiladi, ikkinchisi esa GPIO liniyasiga ulanadi, bu esa mikrokontrollerni uzilish orqali uyqu rejimidan uyg‘otish imkonini beradi.

• Antenna ulagichi: Antenna ulagichi tashqi antennani plataga ulash imkonini beradi.

• XBee tartibi: OpenMote XBee forma faktoriga to‘liq mos keladi, ya’ni XBee Explorer dongle yordamida kompyuter bilan osongina interfeysga kirishi mumkin.

5.5-jadvalda Open Mote, komponentlarning o‘zaro ta’siri va ulagichlar bilan mavjud sensorlarning sxematik ko‘rinishi berilgan. OpenMote Contiki, OpenWSN, FreeRTOS va RiOT kabi bir nechta operatsion tizimlarni boshqaradi. Uni 0-sinf cheklangan qurilmalar sifatida tasniflash mumkin.

1.5-jadval

OpenMote platformasining qurilmaviy tavsifi

Name	Description
MCU	TI 32-bit Cortex-M3
RAM	32 kB
ROM	512 kB
Digital communication	I2C, and UART
Main module current draw	0.5 mA (active mode)
	0.5 μA (standby mode)
IEEE 802.15.4 compliant	
RF transceiver	CC2520 2.4 GHz
Battery	2 × AAA cells
Sensors	Temperature/humidity sensor (SHT21)
	Acceleration sensor (ADXL346)
	Light sensor (MAX44009)

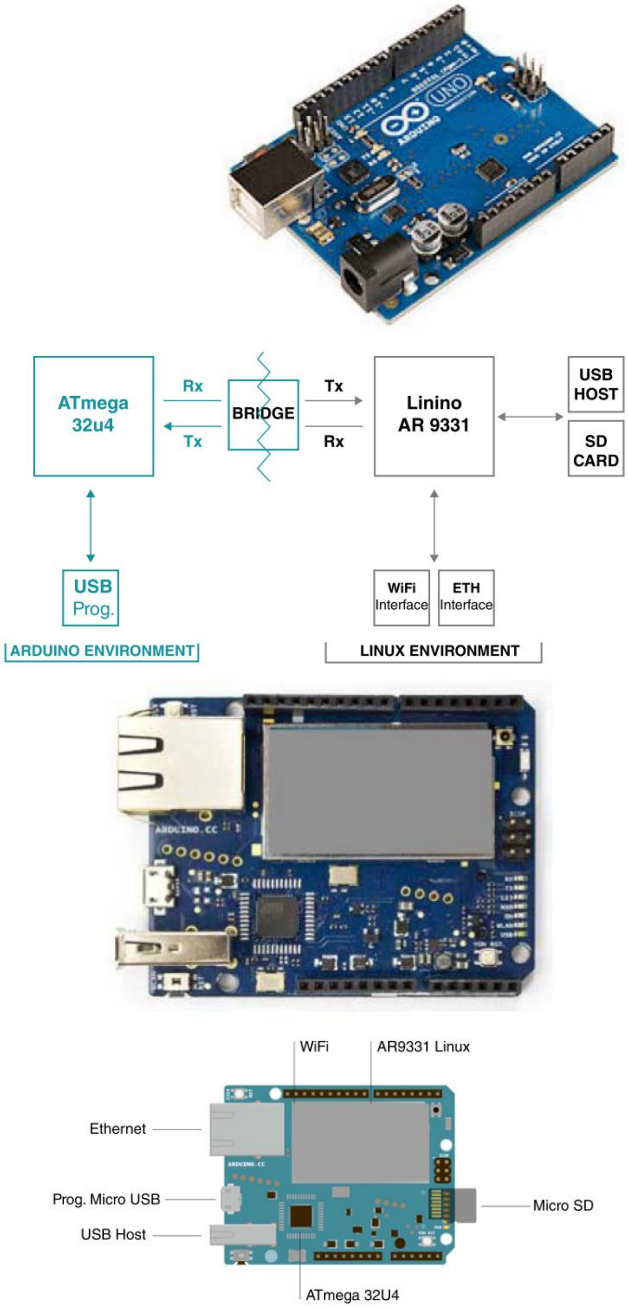
Arduino

Arduino - bu fizik dunyoni sezadigan va o‘zaro aloqada bo‘ladigan raqamli qurilmalarni yaratish uchun mikrokontroller to‘plamlarini ishlab chiqaradigan kompyuter apparat va dasturiy ta’minot kompaniyasi. Plata loyihalari turli xil mikroprotsessorlar va kontrollerlarni qabul qiladi va raqamli va analogli kirish / chiqish pinlari to‘plamlari bilan jihozlangan bo‘lib, ular interfeysli kengaytirish platalari (“qalqon” deb ataladi) va boshqa tashqi sxemalar va komponentlar bo‘lishi mumkin. Oddiy dasturlash tili an’anaviy C va C++ dialekti bo‘lib, ishlab chiquvchilar tomonidan yaratilgan mavjud ko‘plab kutubxonalarni qo‘shish imkoniyatiga ega. Arduino loyihasi 2005-yilda Italiyada Ivrea Interaction Design Institute talabalari uchun dastur sifatida boshlangan. Maqsad yangi boshlovchilar va professionallar uchun arzon va foydalanish uchun qulay platani yaratish edi. Arduino platalari sensorlar va bajaruvchi mexanizmlar va bir nechta aloqa paradigmalaridan foydalangan holda atrof-muhit bilan o‘zaro ta’sir qiluvchi qurilmalar va prototiplarni yaratish uchun mo‘ljallangan (qalqonni kengaytirish platalari tizimi tufayli).

IoT ekotizimlari uchun qurilgan birinchi Arduino platalaridan biri Arduino Yun edi. Bu ATmega32u4 va Atheros AR9331 ga asoslangan mikrokontroller platasi. Atheros protsessori Linino OS deb nomlangan OpenWrt 5-ga asoslangan Linux distributivida ishlaydi. Platada o‘rnatilgan Ethernet va Wi-Fi aloqa interfeyslari, USB-A porti, micro-SD karta porti, 20 ta raqamli kirish/chiqish pinlari (ulardan yettitasi PWM chiqishi va o‘n ikkitasi analog kirish sifatida ishlatilishi mumkin), 16 MGts kristall osilator, mikro USB ulanishi, ICSP sarlavhasi va uchta reset tugmasi.

1.3-rasmda Arduino Yun arxitekturasi va panelning Linux moduli an’anaviy Arduino moduli bilan qanday bog‘lanishi ko'rsatilgan. Ushbu aloqa qobiliyati platani boshqa platalardan ajratib turadi va bir nechta dastur ssenariylarida IoT prototiplarini yaratish uchun ishlatilishi mumkin bo‘lgan kuchli tarmoqqa ulangan

kompyuterni taklif qiladi.



1.3-rasm. Arduino platformasining klassik va Yun versiyalari, Yun apparat arxitekturasi va asosiy komponentlari batafsil tavsifi

1.6 va 1.7-jadvallarda Arduino Yun modullarining tegishli komponentlari va tavsiflari bilan batafsil apparat profili keltirilgan. Yun platasini 2-sinf cheklangan qurilma sifatida tasniflash mumkin.

1.6-jadval

Arduino Yun AVR Arduino mikrokontrollerining apparat spetsifikatsiyasi

Name	Description
Microcontroller	ATmega32U4
Operating Voltage	5 V
Input Voltage	5 V
Digital I/O pins	20
PWM Output	7
Analog I/O pins	12
Flash memory	32 kB (4 kB used by the bootloader)
SRAM	2.5 kB
EEPROM	1 kB
Clock speed	16 MHz

1.7-jadval

Arduino Yun Arduino mikroprotsessorining apparat spetsifikatsiyasi

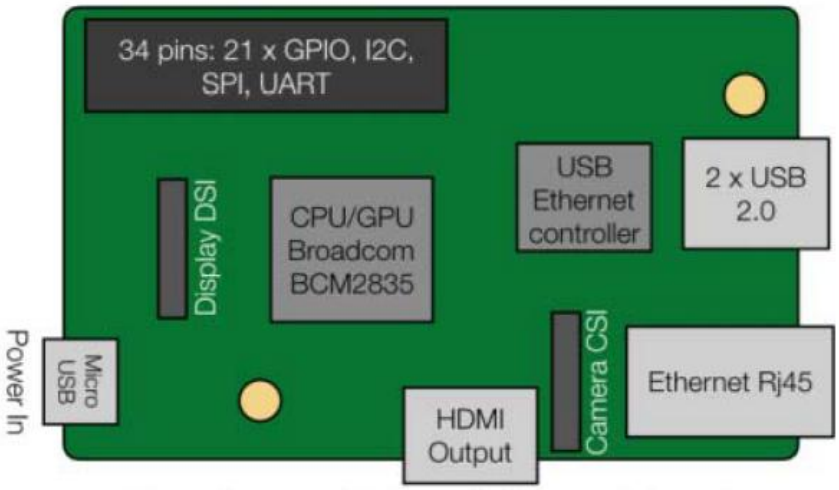
Name	Description
Processor	Atheros AR9331
Architecture	MIPS
Operating voltage	3.3 V
Ethernet	IEEE 802.3 (10/100Mbit/s)
Wi-Fi	IEEE 802.11b/g/n (2.4 GHz)
USB type	2.0 Host
Flash memory	16 MB
RAM	64 MB DDR2
SRAM	2.5 kB
EEPROM	1 kB
Clock speed	400 MHz

Raspberry Pi

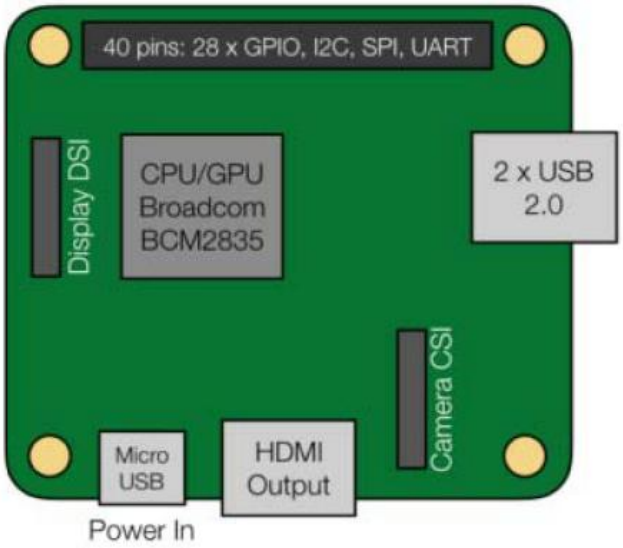
Raspberry Pi - Buyuk Britaniyada Raspberry Pi fondi tomonidan yaratilgan bir platali kompyuter seriyasi. Ta’sischilarning asl maqsadi maktablarda va rivojlanayotgan mamlakatlarda asosiy kompyuter fanlarini o‘qitishni rag‘batlantirish edi. Bosqichma-bosqich, ularning kengashlari ishlab chiqaruvchilar va ishlab chiquvchilarning ko‘plab dastur ssenariylarida yangi loyihalar haqida o‘ylash va yaratish usullarini sezilarli darajada o‘zgartirdi. Misol uchun, original model juda mashhur bo‘ldi va robototexnika kabi foydalanish uchun dastlabki maqsadli bozoridan tashqarida tarqala boshladi.

1.4-rasmda uchta Raspberry Pi platalarida mavjud komponentlar va apparat profillari ko‘rsatilgan. Broadcom BCM2835 SoC plataning birinchi avlodida ishlatilgan va birinchi avlod smartfonlarida ishlatiladigan chipdan foydalanilgan (uning protsessori eski ARMv6 arxitekturasi). U 700 MGts chastotali ARM1176JZF-S protsessorini, VideoCore IV GPU va operativ xotirani o‘z ichiga oladi. Uning 1-darajali (L1) keshi 16 kB va 2-darajali (L2) keshi 128 kB. 2-darajali

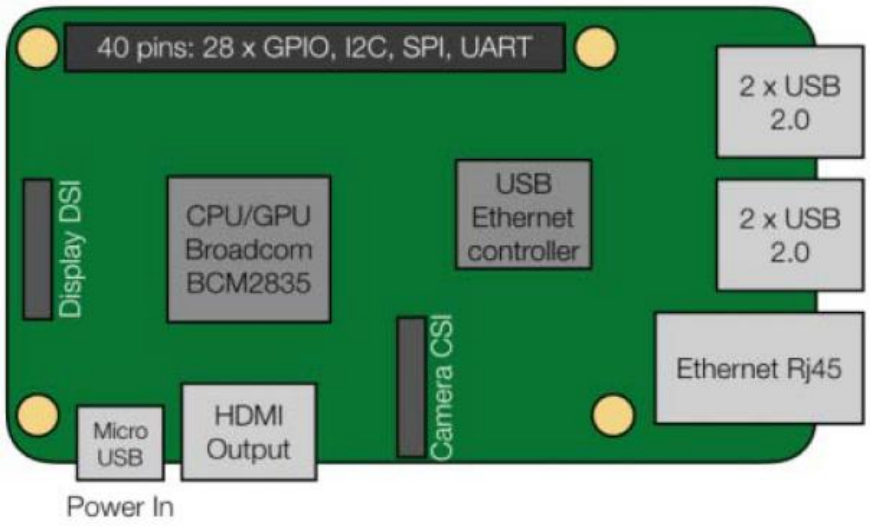
kesh asosan GPU tomonidan qo‘llaniladi. SoC RAM chipi ostiga joylashtirilgan, shuning uchun faqat uning chetki qismi ko‘rinadi.



Raspberry Pi 1 model B revision 2



Raspberry Pi 1 model A+ revision 1.1



Raspberry Pi 1 model B+ revision 1.2 and Raspberry Pi 2 model B

1.4-rasm. Asosiy Raspberry Pi platalari va uning versiyalari

Raspberry Pi 2 900 MGts chastotali 32 bitli to‘rt yadroli ARM Cortex-A7

protsessoriga ega Broadcom BCM2836 SoCdan foydalanadi (ko‘plab hozirgi smartfonlar kabi), umumiy L2 keshi 256 kB.

Raspberry Pi 3 1,2 gigagersli 64 bitli to‘rt yadroli ARM Cortex-A53 protsessoriga ega, 512 kB umumiy L2 keshiga ega Broadcom BCM2837 SoCdan foydalanadi.

Model A, A+ va Pi Zero Ethernet modullariga ega emas va odatda Ethernet yoki Wi-Fi uchun tashqi adapterlar yordamida tarmoqqa ulanadi. B va B+ modellarida SMSC LAN9514 chipi yordamida o‘rnatilgan USB Ethernet adapteri bilan ta’minlangan chekilgan port mavjud. Raspberry Pi 3 va Pi Zero W (simsiz) 2,4 gigagersli Wi-Fi 802.11n (150 Mbit/s) va Bluetooth 4.1 (24 Mbit/s) ulanish modulini Broadcom BCM43438 chipi asosida taqdim etadi. Raspberry Pi 3 shuningdek, 10/100 Ethernet porti bilan jihozlangan.

Raspberry Pi-dan USB xotirasi, USB-dan MIDIga o‘zgartirgichlar va USB imkoniyatlariga ega deyarli har qanday boshqa qurilma/komponent bilan ham foydalanish mumkin. Boshqa tashqi qurilmalar, sensorlar/boshqaruv mexanizmlari va tashqi qurilmalar plata yuzasida mavjud bo‘lgan pinlar va ulagichlar to‘plami orqali ulanishi mumkin.

Raspberry Pi platalar oilasi Raspbian, Fedora, Ubuntu MATE, Kali Linux, Ubuntu Core, Windows 10 IoT Core, RISC OS, Slackware, Debian, Arch Linux ARM va Android Things kabi bir nechta operatsion tizimlarni ishga tushirishi mumkin. Yuqori profilli apparat, dasturiy ta’minot va operatsion tizimlarning bunday kombinatsiyasi ushbu platalarni geterogen IoT ilovalarida kuchli va murakkab tugunlarni ifodalashga imkon beradi. Ular geterogen protokollardan foydalangan holda IoT markazlari, shlyuzlar va ma’lumotlar yig‘uvchilar sifatida samarali ishlashi va bir vaqtning o‘zida bir nechta xizmatlarni ishga tushirishi mumkin. Barcha Raspberry Pi platalarini 2-sinf cheklangan qurilmalar sifatida tasniflash mumkin.

IoT uchun dasturiy vositalar

Ushbu bo‘limda IoT uchun asosiy operatsion tizimlar haqida umumiy ma’lumot berilgan. Contiki operatsion tizimi ayniqsa muhim bo‘lib, quyida keltirilgan.

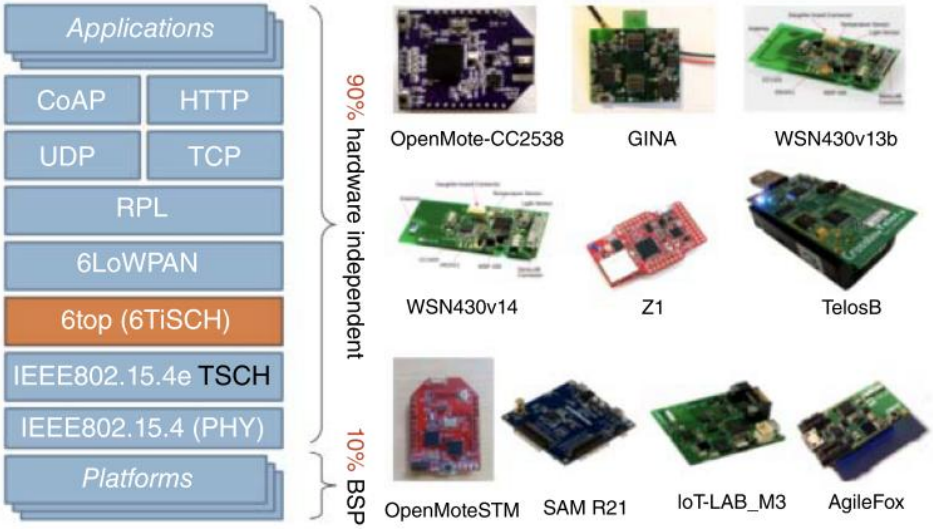
OpenWSN

OpenWSN loyihasi IoT tarmoqlari uchun to‘liq standartlarga asoslangan protokollar stekining ochiq manbali amalga oshirilishidir. U yangi IEEE802.15.4e vaqt oralig‘idagi kanallarni o‘tish standartiga asoslangan. IEEE802.15.4e 6LoWPAN, RPL va CoAP kabi IoT standartlari bilan birgalikda Internetga to‘liq integratsiyalangan juda kam quvvat sarflaydigan va yuqori ishonchli tarmoqli tarmoqlarni yaratish imkonini beradi.

OpenWSN eski 16-bitli mikro-kontrollerlardan eng zamonaviy 32-bitli Cortex-M arxitekturalariga qadar ko‘plab tijorat platformalariga o‘tkazildi. OpenWSN loyihasi protokollar to‘plamini va uning atrofidagi debaggerlash va integratsiya vositalarini bepul va ochiq manbali amalga oshirishni taklif qiladi va shu bilan kam quvvatli simsiz tarmoq tarmoqlaridan foydalanishni rag‘batlantirishning umumiy maqsadiga hissa qo‘shadi.

1.5-rasmda apparatdan mustaqil bo‘lgan OpenWSN protokoli qatlamlari va

dasturiy ta’minot kutubxonalari hamda ularni o‘rnatish va ishlatish mumkin bo‘lgan qo‘llab-quvvatlanadigan apparat platformalari to‘plami ko‘rsatilgan.



1.5-rasm. Uskunadan mustaqil modullar va qo‘llab-quvvatlanadigan apparat platformalarini ajratib ko‘rsatadigan OpenWSN protokoli to‘plami

TinyOS

TinyOS bu bepul, ochiq manbali, BSD-litsenziyali operatsion tizim bo‘lib, sensorli tarmoqlarda ishlatiladigan kam quvvatli o‘rnatilgan taqsimlangan simsiz qurilmalar uchun mo‘ljallangan. U minimal apparat talablari bilan tarmoqqa ulangan sensorlar tomonidan talab qilinadigan intensiv bir vaqtda operatsiyalarni qo‘llab-quvvatlash uchun mo‘ljallangan. TinyOS Kaliforniya universiteti, Berkli, Intel Research va Crossbow Technology tomonidan ishlab chiqilgan. U nesC (Network Embedded Systems C) dasturlash tilida yozilgan bo‘lib, u komponentlar va parallellikni qo‘llab-quvvatlash uchun optimallashtirilgan C versiyasidir. Bu, shuningdek, komponentlarga asoslangan bo‘lib, TinyOS uchun ilovalarni hodisalarga (event-driven) asoslangan dasturlashni qo‘llab-quvvatlaydi.

FreeRTOS

FreeRTOS - bu kichik va oddiy bo‘lishi uchun mo‘ljallangan o‘rnatilgan qurilmalar uchun real vaqtda operatsion tizim yadrosi. U 35 ta mikro-kontrollerga o‘rnatilgan va ixtiyoriy istisno bilan GPL litsenziyasi ostida tarqatiladi. Istisno foydalanuvchilarning xususiy kodi yopiq manba bo‘lib qolishiga imkon beradi, shu bilan birga yadroning o‘zini ochiq manba sifatida saqlaydi va shu bilan xususiy ilovalarda FreeRTOSdan foydalanishni osonlashtiradi.

Kodni o‘qish, kodni yangilashni osonlashtirish va texnik xizmat ko‘rsatish uchun u asosan C tilida yozilgan (lekin ba’zi yig‘ish funktsiyalari arxitekturaga xos rejalashtiruvchi tartiblarni qo‘llab-quvvatlash uchun kiritilgan). U bir nechta mavzular yoki vazifalar, mutekslar, semaforlar va dasturiy ta’minot taymerlari uchun usullarni taqdim etadi.

Contiki OS

Contiki - kam quvvatli simsiz IoT qurilmalariga mo‘ljallangan tarmoqqa ulangan, xotirasi cheklangan tizimlar uchun operatsion tizim. Uning asosiy xususiyatlari quyida keltirilgan:

• Bu ochiq manba va doimiy rivojlanishda. Tijoriy operatsion tizimlarga

qaraganda kamroq hujjatlashtirilgan va unchalik yaxshi saqlanmagan bo‘lsa ham, u ishlab chiquvchilarga nafaqat maxsus ilovalar ustida ishlash, balki TCP/IP stek va marshrutlash protokoli kabi asosiy OT funksiyalarini o‘zgartirish imkonini beradi.

• Sarlavhani siqish uchun 6LoWPAN yordamida to‘liq TCP/uIPv6 stekini taqdim etadi va RPL bilan LR-WPAN marshrutlarini yaratadi. Kam quvvat sarflaydigan va yo‘qotishli tarmoqlar uchun IPv6 marshrutlash protokolidan foydalanadi.

Contiki 2002-yilda Adam Dunkels tomonidan yaratilgan va Texas Instruments, Atmel, Cisco, ENEA, ETH Zurich, Redwire, RWTH Aachen universiteti, Oksford universiteti, SAP, Sensinode, Shvetsiya Kompyuter fanlari instituti, ST Microelectronics, Zolertia va boshqa kompaniyalarning butun dunyo bo‘ylab ishlab chiquvchilari jamoasi tomonidan ham ishlab chiqilgan.

Contiki xotira, quvvat, ishlov berish quvvati va aloqa o‘tkazish qobiliyati jihatidan jiddiy cheklangan apparat qurilmalari sinflarida ishlash uchun mo‘ljallangan. Misol uchun, xotira nuqtai nazaridan, ko‘p vazifali va o‘rnatilgan TCP/IP stekini ta’minlaganiga qaramay, Contiki uchun faqat 10 kB RAM va 30 kB ROM kerak. Oddiy Contiki tizimi kilobaytlar tartibini xotirasiga, millivatt quvvat byudjetiga, megagertsda o‘lchanadigan ishlov berish tezligiga va yuzlab kilobit/ sekundgacha bo‘lgan aloqa o‘tkazish qobiliyatiga ega. Ushbu toifadagi tizimlar har xil turdagi o‘rnatilgan tizimlarni va bir qator eski 8 bitli kompyuterlarni o‘z ichiga oladi.

1.3. Ananaviy kriptografik algoritmlarni amalga oshirishdagi muammolar

Klassik shifrlash algoritmlari, masalan, DES (Data Encryption Standard) va AES (Advanced Encryption Standard), IoT uchun aslida nomaqbul tanlov emas; ammo, IoT qurilmalari uchun o‘ziga xos cheklovlar va talablar tufayli ularni to‘g‘ridan-to‘g‘ri IoT muhitida qo‘llash muammolarga duch kelishi mumkin. Quyida ushbu muammolarni ilmiy ma'lumotlar asosida batafsil tahlil qilish keltirilgan:

Klassik shifrlash algoritmlari, masalan, DES (Data Encryption Standard) va AES (Advanced Encryption Standard), IoT uchun aslida nomaqbul emas; ammo, IoT qurilmalari uchun o‘ziga xos cheklovlar va talablar tufayli ularni to‘g‘ridan-to‘g‘ri IoT muhitida qo‘llash muammolarga duch kelishi mumkin. Quyida ushbu muammolarni ilmiy ma'lumotlar asosida batafsil tahlil qilish keltirilgan:

1. IoT qurilmalarining resurs cheklovlari

IoT qurilmalari ko‘pincha cheklangan hisoblash quvvati, xotira va energiya sig‘imiga ega. An’anaviy shifrlash algoritmlari, xususan, 128-bit yoki undan yuqori kalit o‘lchamlariga ega AES, hisoblash uchun juda ko‘p resurs talab qiladi.

Masalan, resurslar cheklangan qurilmalarda AES ni amalga oshirish yuqori kechikish va yuqori energiya iste’moliga olib keladi. Masalan, 16-bitli mikrokontrollerda AES-128 shifrlash energiya iste’moli qurilmaning umumiy quvvat hajmining 70% gacha bo‘lishi mumkin, bu esa batareyadan quvvat oluvchi IoT qurilmalari uchun to‘g‘ri kelmaydi.

2. Kechikish va real vaqt rejimida ishlash

Ko‘plab IoT ilovalari real vaqt yoki real vaqtga yaqin ma’lumotlarni qayta

ishlashni talab qiladi. AES kabi algoritmlar bir necha bosqichli hisoblashlarni o‘z ichiga oladi (AES-128 uchun 10 bosqich, AES-192 uchun 12 bosqich va h.k.), bu esa nojoiz kechikishlarga olib kelishi mumkin.

Masalan, quvvati past IoT qurilmasida AES-256 shifrlashning kechikishi bir operatsiya uchun 15 ms dan oshadi. Bu sanoat avtomatizatsiyasi yoki sog‘liqni saqlash monitoringi kabi kechikish 5 ms dan kam bo‘lishi kerak bo‘lgan ilovalar uchun juda sekin hisoblanadi.

3. Aloqa yuklamasi

IoT tarmoqlari ko‘pincha kichik ma’lumot paketlarini uzatadi. DES, AES va shunga o‘xshash blok shifrlari belgilangan o‘lchamdagi bloklarda ishlaydi (masalan, DES uchun 64 bit, AES uchun 128 bit). Agar ma’lumot blok o‘lchamidan kichik bo‘lsa, padding (to‘ldirish) uzatilgan ma’lumot hajmini oshiradi va samaradorlikni pasaytiradi.

Masalan, AES shifrlash padding va blokni moslashtirish sababli paket hajmini 30% gacha oshiradi, bu esa LPWAN (Low Power Wide Area Networks) kabi cheklangan IoT tarmoqlarida ko‘proq tarmoq o‘tkazuvchanligini talab qiladi.

4. Kalitlarni boshqarish muammolari

DES va AES kabi simmetrik shifrlash algoritmlari xavfsiz kalit almashish va boshqarishni talab qiladi. IoT muhitlari ko‘pincha minglab qurilmalardan iborat bo‘ladi, bu esa markazlashgan kalit boshqarishni murakkablashtiradi va qimmatlashtiradi.

Masalan, IoT tarmoqlarida simmetrik kalit boshqarish hajmini kengaytirish hujum sohasini va operatsion murakkablikni oshiradi, bunda kalitlarni qayta ishlatish va noto‘g‘ri saqlash kabi zaifliklar muhim xavfga aylanadi.

5. Fizik hujumlarga zaiflik

IoT qurilmalari himoyasiz muhitlarda joylashtiriladi, bu yerda hujumchilar qo‘shimcha kanallar orqali (masalan, quvvat tahlili yoki vaqt tahlili hujumlari) shifrlash algoritmlaridan kalitlarni chiqarib olishlari mumkin.

Masalan, IoT qurilmalaridagi AES implementatsiyalari quvvat tahlili hujumlariga zaif. Masalan, hujumchi odatiy mikrokontrollerlarda 1,000 ta quvvat izidan kam foydalanib to‘liq AES-128 kalitini olish imkoniyatiga ega.

6. Tahdidlar salmog‘ining ortishi

IoT qurilmalari o‘ziga xos tahdid modellariga mo‘ljallangan yengil shifrlash yechimlarini talab qiladi. DES kichik kalit o‘lchami (56 bit) tufayli eskirgan, AES esa xavfsiz bo‘lsada, o‘ta muhim bo‘lmagan ma’lumotlar uchun ortiqcha bo‘lishi mumkin va tez-tez yangilanish talablariga javob bermasligi mumkin.

Masalan, NIST Lightweight Cryptography loyihasi (2023) IoT uchun optimallashtirilgan yengil shifrlash algoritmlariga bo‘lgan ehtiyojni ta’kidlab, AES-CCM (yengil variant) yoki Ascon kabi yangi shifrlar misol sifatida keltirilgan.

IoT muhitlari uchun Ascon, SPECK va SIMON (NSA tomonidan cheklangan qurilmalar uchun ishlab chiqilgan) kabi yengil shifrlash algoritmlari yoki AESning moslashtirilgan versiyalari (masalan, AES-CTR yoki AES-CCM) yaxshiroq mos keladi. Ushbu algoritmlar quyidagilarni ta’minlaydi:

Hisoblash murakkabligini kamaytirish.

Energiya iste’molini pasaytirish.

Kichik xotira hajmini talab qiladi.

IoT uchun mos bo‘lgan yetarli darajadagi xavfsizlikni ta’minlaydi.

Moslashtirilgan shifrlash yondashuvlarini qabul qilish orqali IoT tarmoqlari xavfsizlik va samaradorlikni muvozanatlashtirishi, IoT tizimlarining kengaytirilishini va samaradorligini ta’minlashi mumkin.

Nazorat savollari:

1. Buyumlar Interneti tushunchasini misollar yordamida tushuntiring?
2. IoT hozirda qaysi sohalarda keng qo‘llanilmoqda?
3. IoT sohasida aqlli obyektni tashkil etuvchilarini ayting?
4. Aqlli ob’ektlar uchun quvvat manbalari va ularning xususiyatlarini ayting?
5. RFC7228da keltirilgan imkoniyati cheklangan qurilmalar sinflarini ayting?
6. IoTda hozirda ishlatiladigan keng tarqalgan apparat platformalar haqida ayting?
7. IoTda hozirda ishlatiladigan keng tarqalgan dasturiy vositalar haqida ayting?
8. Ananaviy kriptografik algoritmlar nima uchun IoT qurilmalariga mos emas?
9. IoT qurilmalari uchun mos kriptografik algoritmlarni yaratishdan asosiy maqsad nima?

Adabiyotlar va Internet resurslar:

1. Cirani S. et al. Internet of things: architectures, protocols and standards. – John Wiley & Sons, 2018.
2. https://datatracker.ietf.org/doc/html/rfc7228 - Terminology for Constrained-Node Networks

2-ma’ruza. YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLAR (2 соат)

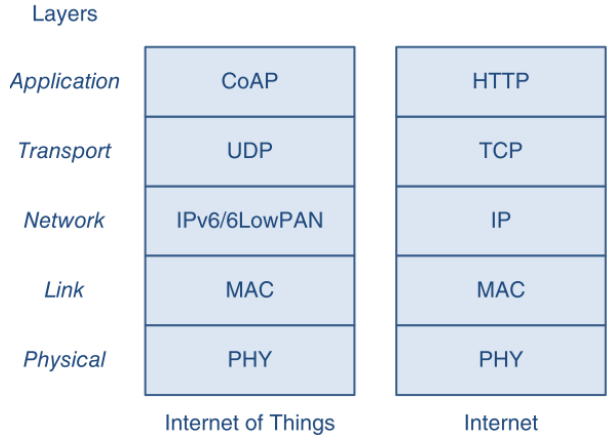
Reja:

2.1. Tarmoq sathlarida foydalanilgan yengil protokollar
2.2. Yengil simmetrik kalitli shifrlash algoritmlar
2.3. Yengil ochiq kalitli kriptografik algoritmlar
2.4. Gomomorfik shifrlash usullari
2.5. Yengil kriptografik protokol: DTLS.

Tayanch iboralar: *CoAP, DTLS, 6LowPAN, TEA, SEA, PRESENT, HIGH, RSA, Elliptik ergi chiziq, PHOTON, SPONGENT, QUARK, Keccak, Gomomorfik shifrlash.*

2.1. Tarmoq sathlarida foydalanilgan yengil protokollar

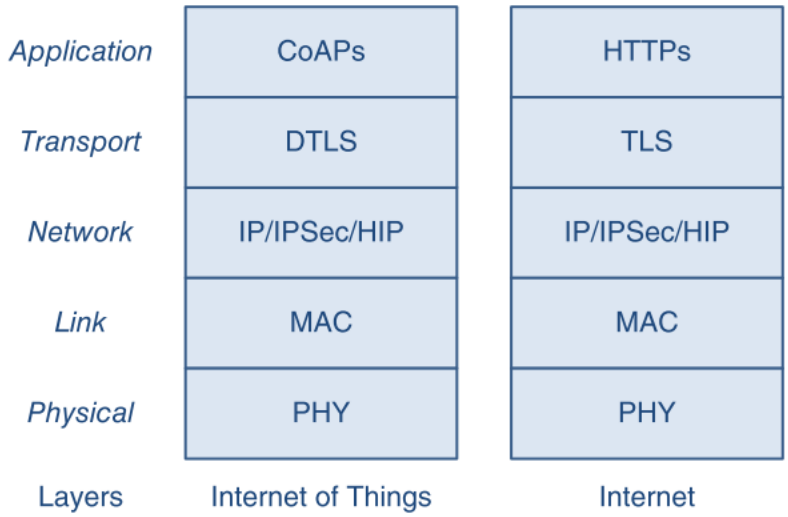
2.1-rasmda odatiy IP-ga asoslangan IoT protokoli stegi tasvirlangan va Internetdan foydalanish uchun standart cheklanmagan tugunlar tomonidan ishlatiladigan klassik Internet protokoli stegi bilan taqqoslanadi. Ilova sathida HTTP protokoli cheklangan dastur protokoli (Constrained Application Protocol, CoAP) bilan almashtiriladi, bu esa resurslar cheklangan qurilmalar tomonidan qo‘llaniladigan amaliy qatlam protokoli hisoblanadi. U mashinadan mashinaga (M2M) aloqa uchun taqdimiy holatni uzatish (representational state transfer, REST) xizmatini taklif qiladi va HTTP ga/dan osongina almashtirilishi qilinishi mumkin.



2.1-rasm. OSI qatlamlari uchun IoT va Internet protokoli stekini taqqoslash

An’anaviy va yengil vaznli xavfsizlik

2.1-rasmda tasvirlangan protokol steklariga ko‘ra, Internet va IoT ssenariylarida xavfsizlik protokollarining mumkin bo‘lgan qatlamli arxitekturalari o‘rtasidagi to‘g‘ridan-to‘g‘ri taqqoslash 2.2-rasmda ko‘rsatilgan.



2.2-rasm. Internet va IoT xavfsizlik protokollarini taqqoslash

Engil vaznli kriptografiya (Lightweight Cryptography, LWC)

IoT ning rivojlanishi mavjud Internet bilan o‘zaro aloqada bo‘ladigan milliardlab aqlli ob’ektlarni joylashtirishga olib keladi. Aqlli ob’ektlar - cheklangan resurslarga ega bo‘lgan kichik hisoblash qurilmalaridir, ya’ni: past hisoblash qobiliyati, kam xotira va cheklangan batareya quvvati.

Resurs cheklangan muhitda aqlli ob’ektlar bilan aloqa qilish, ayniqsa xavfsizlik muhim bo‘lgan va AES kabi an’anaviy kriptografik shifrlar etarli bo‘lmagan ssenariylarda ushbu qattiq cheklovlarni albatta hisobga olishi kerak.

Yengil vaznli kriptografiya (LWC) - bu aqlli ob’ektlar talablariga javob beradigan yangi shifrlarni loyihalashga qaratilgan juda qiziqarli tadqiqot sohasi. “Yengil vaznli” atamasini “zaif” degan ma’no sifatida (kriptografik himoya nuqtai nazaridan) noto‘g‘ri tushunmaslik kerak, aksincha, kichikroq hajmga ega kriptografik algoritmlar oilasiga ishora sifatida talqin qilinishi kerak, ya’ni, energiya sarfi kamroq va hisoblash quvvati kam. Ushbu shifrlar ko‘plab qurilmalarda uchraydigan cheklangan resurslar muhitida etarli xavfsizlikni ta’minlashga qaratilgan. Shunday qilib, LWC cheklangan qurilmalarga moslashtirilgan kriptografiyani ifodalaydi, bu xavfsizlik darajasi, xarajat va unumdorlik o‘rtasidagi o‘zaro kelishuvga javob berishi kerak.

2.2. Yengil simmetrik kalitli shifrlash algoritmlar

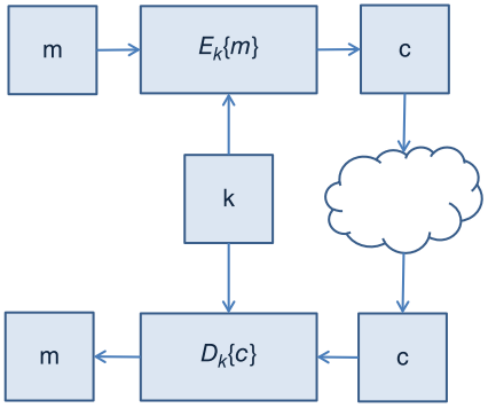
Simmetrik kalitli LWC algoritmlar

Simmetrik kalitli kriptografik algoritmlar ochiq matnni shifrlash va shifrlangan matnni deshifrlash uchun bir xil kalitdan foydalanadi. Shifrlash kaliti xavfsiz aloqada ishtirok etuvchi tomonlar o‘rtasidagi umumiy maxfiy kalitni ifodalaydi. Simmetrik kalitli xavfsiz aloqaning ko‘rinishi 2.3-rasmda ko‘rsatilgan.

Simmetrik kalitli shifrlash blokli shifrlardan ham, oqimli shifrlardan ham foydalanishi mumkin:

Blokli shifrlar bloklar deb ataladigan belgilangan uzunlikdagi bit guruhlarida ishlaydi va ochiq matn uzunligini blok o‘lchamining ko‘paytmasiga teng qilish uchun to‘ldiradi. Misol tariqasida AES algoritmini keltirish mumkin.

Oqimli shifrlarda ochiq matn bitlari bir vaqtning o‘zida psevdo tasodifiy ketma-ketliklar oqimning (kalitlar oqimi) mos keladigan bitlari bilan shifrlanadi.



2.3-rasm. Simmetrik kalitli kriptografik algoritmlar bilan xavfsiz aloqa

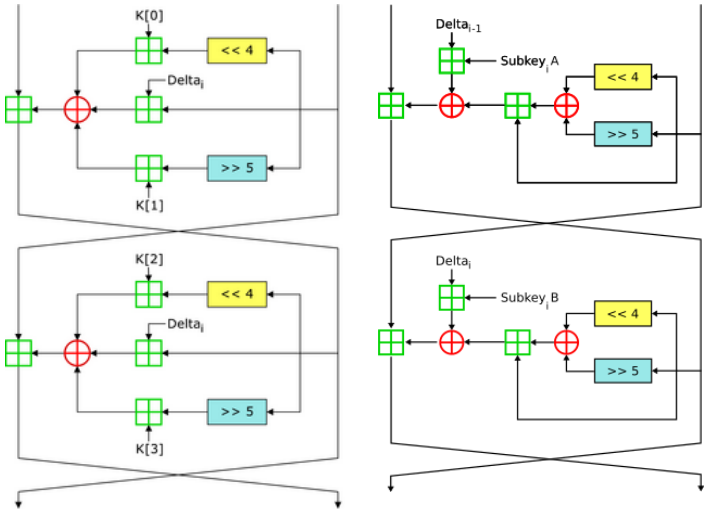
Tiny Encryption Algoritm

Tiny Encryption Algoritm (TEA) blokli shifr bo‘lib, tavsif va amalga oshirishning soddaligi bilan mashhur; odatda bir necha qator kodlar orqali amalga oshirish mumkin. TEA ikkita 32-bitli unsigned tipidagi butun sonlarda ishlaydi (ular 64-bitli ma’lumotlar blokidan olinishi mumkin) va 128-bitli kalitdan foydalanadi. TEA faqat 32 bitli so ‘zlar ustidagi arifmetik amallarga tayanadi va faqat qo‘shish, XORlash va siljishlardan foydalanadi. TEA oldindan belgilangan jadvallar va uzoq vaqtda amalga oshiriluvchi amallarning o‘rniga sodda amallardan ko‘p sonli iteratsiyalarda foydalanishga asoslanadi. TEA ning asosiy loyihalash maqsadi oldindan o‘rnatilgan jadvallar yoki oldindan hisob-kitoblarga tayanmaydigan oddiy va qisqa shifrni aniqlashdan iborat bo‘lib, bu kam sonli mantiqiy elementlardan iborat qurilmani yaratishga imkon beradi.

TEA original algoritmda topilgan ba’zi zaif tomonlarni tuzatish uchun qayta ko‘rib chiqildi, masalan, ekvivalent kalitlar muammosi, bu kalitning haqiqiy hajmini 128 dan 126 bitgacha qisqartirdi. XTEA (kengaytirilgan TEA) deb nomlangan TEA ning qayta ko‘rib chiqilgan loyihasi asosiy jadvalni o‘zgartirish orqali bu muammoni hal qiladi. XTEA shuningdek, ikkita kamroq qo‘shimchani talab qiladi, shuning uchun algoritm biroz tezroq ishlaydi. TEA algoritmining boshqa modifikatsiyalari, masalan, XXTEA, blokli TEA, tezkor TEA va kichik XTEA kabilar taqdim etilgan.

TEA oilasi juda oddiy operatsiyalardan foydalanganligi va juda kichik kod hajmiga ega bo‘lganligi sababli, u aqlli ob’ektlar va simsiz sensorlarda xavfsizlik mexanizmlarini amalga oshirish uchun kriptografik algoritm sifatida ideal nomzodlar hisoblanadi.

2.4-rasmda TEA va XTEA algoritmlarining shifrlash sxemalari keltirilgan. Ularning C dasturlash tilidagi ifodasi esa quyida keltirilgan.



2.4-rasm. TEA va XTEA algoritmlarining shifrlash sxemalari

TEA algoritmining C dasturlash tilidagi kodi:

```
#include <stdint.h>

void encrypt (uint32_t v[2], const uint32_t k[4]) {
    uint32_t v0=v[0], v1=v[1], sum=0, i;           /* set up */
    uint32_t delta=0x9E3779B9;                     /* a key schedule
constant */
    uint32_t k0=k[0], k1=k[1], k2=k[2], k3=k[3];   /* cache key */
    for (i=0; i<32; i++) {                         /* basic cycle
start */
        sum += delta;
        v0 += ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
        v1 += ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
    }                                              /* end cycle
*/
    v[0]=v0; v[1]=v1;
}

void decrypt (uint32_t v[2], const uint32_t k[4]) {
    uint32_t v0=v[0], v1=v[1], sum=0xC6EF3720, i;  /* set up; sum
is (delta << 5) & 0xFFFFFFFF */
    uint32_t delta=0x9E3779B9;                     /* a key schedule
constant */
    uint32_t k0=k[0], k1=k[1], k2=k[2], k3=k[3];   /* cache key */
    for (i=0; i<32; i++) {                         /* basic cycle
start */
        v1 -= ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
        v0 -= ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
        sum -= delta;
    }                                              /* end cycle
*/
    v[0]=v0; v[1]=v1;
}
```

XTEA algoritmining C dasturlash tilidagi kodi:

```
#include <stdint.h>
/* take 64 bits of data in v[0] and v[1] and 128 bits of key[0] -
key[3] */

void encipher(unsigned int num_rounds, uint32_t v[2], uint32_t
const key[4]) {
    unsigned int i;
    uint32_t v0=v[0], v1=v[1], sum=0, delta=0x9E3779B9;
    for (i=0; i < num_rounds; i++) {
        v0 += (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum + key[sum &
3]);
        sum += delta;
        v1 += (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum>>11)
& 3]);
    }
    v[0]=v0; v[1]=v1;
}

void decipher(unsigned int num_rounds, uint32_t v[2], uint32_t
const key[4]) {
    unsigned int i;
    uint32_t      v0=v[0],      v1=v[1],      delta=0x9E3779B9,
sum=delta*num_rounds;
    for (i=0; i < num_rounds; i++) {
        v1 -= (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum>>11)
& 3]);
        sum -= delta;
        v0 -= (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum + key[sum &
3]);
    }
    v[0]=v0; v[1]=v1;
}
```

Scalable Encryption Algoritm

Scalable Encryption Algoritm (SEA) kichik o‘rnatilgan ilovalarga mo‘ljallangan. Loyiha juda cheklangan qayta ishlash resurslari va o‘tkazish qobiliyati talablari bo‘lgan muhitni inobatga olib ishlab chiqilgan. SEA ning yana bir loyihalash printsipi moslashuvchanlikdir: ochiq matn o‘lchami n, kalit o‘lchami n va protsessor (yoki so‘z) o‘lchami b loyihalashdagi parametrlar bo‘lib, yagona cheklov n soni $6b$ ga karrali bo‘lishidir; shuning uchun algoritm $SEA_{n,b}$ deb belgilanadi. Ushbu moslashuvchanlikning motivatsiyasi ko‘plab shifrlash algoritmlarining platformaga, masalan, 8-bit yoki 32-bitli protsessorlarga qarab turlicha ishlashini anglatadi. $SEA_{n,b}$ umumiy bo‘lishi va turli xil xavfsizlik darajalariga (kalit o‘lchamini o‘zgartirish orqali) va maqsadli qurilmaga moslash uchun mo‘ljallangan. $SEA_{n,b}$ ning katta afzalligi bu “on-the-fly” kalit yetkazib berilishidadir. Asosiy kamchilik shundaki, $SEA_{n,b}$ vaqtdan samaraga erishish uchun qurilmaning fizik hajmini kengaytiradi va bu cheklangan hisoblash quvvatiga ega qurilmalarda ahamiyatsiz bo‘lishi mumkin emas.

PRESENT shifri

PRESENT - SP tarmog‘iga asoslangan o‘ta engilvaznli blokli shifrlash algoritmi. PRESENT juda ixcham va apparatda samarali bo‘lishi uchun yaratilgan. U 64 bitli bloklarda va 80 yoki 128 bitli kalitlar bilan ishlaydi. U kam quvvat istemoli va yuqori chip samaradorligi talab qilinadigan holatlarda foydalanish uchun mo‘ljallangan, shuning uchun uni cheklangan muhitlar uchun alohida ahamiyatga ega. PRESENT-ning asosiy loyihalash maqsadi, boshqa engil shifrlarda bo‘lgani kabi, soddalikdir. PRESENT 31 raundda amalga oshiriladi, ularning har biri uch bosqichdan iborat (2.5-rasm):

• kalit bilan aralashtirish: XOR amali bo‘yicha qo‘shish va shundan so‘ng kalitni 61-bitli aylantirish orqali kalitlarni yangilash;

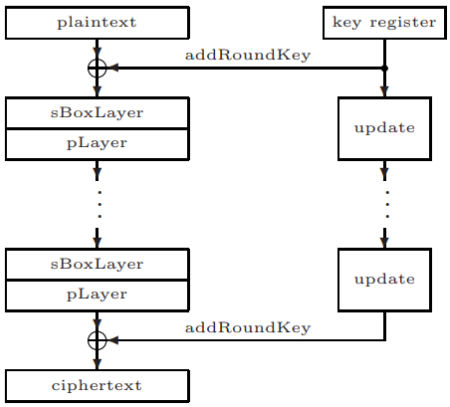
• o‘rniga qo‘yish qatlami, 16 ta 4-bitli (kirish) 4-bitli (chiqish) S jadvallari orqali;

• o‘rin almashtirish qatlami.

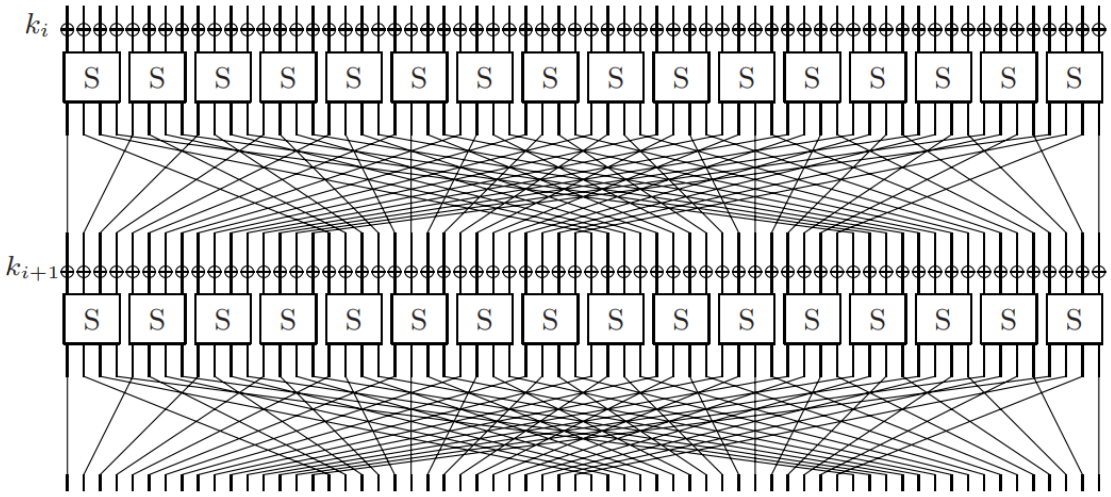
31-raund oxirida qo‘shimcha raund oxirgi raundning qism kalitini XORlash orqali amalga oshiriladi.

Algoritm qabul qilingan *ISO/IEC 29192-2:2012 Lightweight Cryptography* nomlari engil vaznli kriptografiya uchun mos blokli shifr sifatida qabul qilingan.

generateRoundKeys()
for $i = 1$ to 31 **do**
  addRoundKey(STATE,K_i)
  sBoxLayer(STATE)
  pLayer(STATE)
end for
addRoundKey(STATE,K_{32})



2.5-rasm. PRESENT algoritmining qisqa ko‘rinishi



2.6-rasm. PRESENT uchun SP tarmoq

31 raundning har biri raund kaliti K_i $(1 \leq i \leq 32)$ bilan XOR amalida

qo‘shish (K_{32} qo‘shimcha raundda ishlatiladi (post-whitening)), bit darajasida chiziqli almashtirish va chiziqsiz akslantirish (S jadval) amallaridan iborat. Chiziqsiz akslantirish bosqichida 4 bitli S jadval har bir raund uchun parallel ravishda 16 marta ishlatiladi.

addRoundKey. Berilgan $K_i = \kappa_{63}^i \dots \kappa_0^i$ $(1 \le i \le 32)$ raund kaliti va joriy holat (STATE) $b_{63} \dots b_0$ da $0 \le j \le 63$ lar uchun addRoundKey quyidagicha bajariladi:

$$b_j \to b_j \oplus \kappa_j^i$$

sBoxlayer. Present algoritmida foydalanilgan S jadval 4 bit kirish va 4 bit chiqishni amalga oshiradi: $F_2^4 \to F_2^4$. S jadvalning 16 sanoq tizimidagi ifodasi quyida keltirilgan:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

sBoxlayer sathi uchun joriy STATE $b_{63} \dots b_0$ - 16 ta $w_{15} \dots w_0$ 4 bitli so‘zlardan iborat, bu yerda, $0 \le i \le 15$ uchun $w_i = b_{4*i+3} \parallel b_{4*i+2} \parallel b_{4*i+1} \parallel b_{4*i}$ va chiqish $S[w_i]$ esa yangilangan holat qiymatlarini taqdim etadi.

pLayer. PRESENT algoritmida foydalanilgan bitlarni almashtirish quyidagi jadvalga berilgan. STATEning i – biti $P(i)$ pozitsiyadagi bitga ko‘chiriladi.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Raund kalitlarni hosil qilish. PRESENT algoritmida kalit uzunligi 80 yoki 128 bitli bo‘ladi. Hozir esa 80 bit kalit holati qarab chiqiladi. Dastlabki kalit K kalit registrida saqlanadi va $k_{79}k_{78} \dots k_0$ shaklida taqdim etiladi. i-raunddagi 64-bitli raund kaliti $K_i = \kappa_{63}\kappa_{62} \dots \kappa_0$ registrda saqlangan kalit K ning joriy qiymatining chap tomondagi 64 bitidan iborat bo‘ladi. Shuning uchun i raundda quyidagiga ega bo‘linadi:

$$K_i = \kappa_{63}\kappa_{62} \dots \kappa_0 = k_{79}k_{78} \dots k_{16}.$$

Raund kaliti K_i ajratilganidan so‘ng, kalit registori $K = k_{79}k_{78} \dots k_0$ quyidagicha yangilanadi:

1. $[\mathrm{k}_{79}\mathrm{k}_{78} \dots \mathrm{k}_1\mathrm{k}_0] = [\mathrm{k}_{18}\mathrm{k}_{17} \dots \mathrm{k}_{20}\mathrm{k}_{19}]$
2. $[\mathrm{k}_{79}\mathrm{k}_{78}\mathrm{k}_{77}\mathrm{k}_{76}] = S[\mathrm{k}_{79}\mathrm{k}_{78}\mathrm{k}_{77}\mathrm{k}_{76}]$
3. $[\mathrm{k}_{19}\mathrm{k}_{18}\mathrm{k}_{17}\mathrm{k}_{16}\mathrm{k}_{15}] = [\mathrm{k}_{19}\mathrm{k}_{18}\mathrm{k}_{17}\mathrm{k}_{16}\mathrm{k}_{15}] \oplus \mathtt{round\_counter}$

Shunday qilib, kalit registori 61 bit chapga aylantiriladi va chapdagi eng chetki 4 bit S jadvaldan o‘tkaziladi va round_counter qiymati i o‘ng tomondan boshlab (Least significant bit, LSB) XOR amalida K kalitning $k_{19}k_{18}k_{17}k_{16}k_{15}$ bitlariga qo‘shiladi.

HIGH shifri

HIGH yuqori darajada xavfsiz va engil vaznli (**HIG**h security and lightweig**HT**, HIGHT) shifrlash algoritmi 64 bit blok, 128 bitli kalit va 32 raundan iborat bo‘lgan umumlashtirilgan Feistel tarmog‘iga asoslangan. HIGHT kam resurs sarfiga ega apparat ko‘rinishida amalga oshirilishni hisobga olgan holda ishlab chiqilgan. HIGHT juda oddiy operatsiyalardan foydalanadi, masalan, XORlash, qo‘shimcha mod 2^8 va bit bo‘yicha aylantirish. HIGHTdagi kalitlar jadvali shunday tuzilganki, qismkalitlar shifrlash va parolni hal qilish bosqichlarida tezda yaratiladi.

Simmetrik LWC algoritmlarini taqqoslash

LWC algoritmlari keng tarqalgan AES kabi mavjud shifrlarni almashtirish uchun mo‘ljallanmagan. Ularning qo‘llanilishi klassik shifrlar samarasiz bo‘lishi mumkin bo‘lgan ssenariylar bilan cheklangan, masalan:

• kalitlar juda uzun bo‘lmasligi uchun o‘rtacha xavfsizlik darajasi talab qilinadi;

• katta hajmdagi ma’lumotlarga shifrlash qo‘llanilmasligi kerak;

• amalga oshirish uchun zarur bo‘lgan apparat maydoni va quvvat sarfi tezlikdan ko‘ra qiyinroq talablar hisoblanadi.

Cheklangan qurilmalar uchun kriptografik algoritmni tanlash ishlashga ta’sir qilishi mumkin bo‘lgan asosiy element hisoblanadi. Kam xarajat va energiya iste’moli qiyin talablar bo‘lsa, hisoblash quvvati tabiiy ravishda mos ravishda qisqartirilishi kerak. Hisoblash quvvati, xotira va saqlash nuqtai nazaridan cheklangan imkoniyatlarga ega bo‘lgan 8-bitli mikrokontrollerlardan (masalan, Atmel AVR mikrokontrollerlari) foydalanish amalga oshirilgan shifrlarning kichik xotiraga ega bo‘lishini va sodda bo‘lishini talab qiladi. Bu tezroq ishlashga va shuning uchun batareyadan quvvat oladigan qurilmalar uchun juda muhim bo‘lgan energiya sarfini kamaytirishga olib kelishi mumkin.

Ko‘pgina simmetrik kriptografik algoritmlar samarali dasturiy ta’minotni amalga oshirishga qaratilgan bo‘lsada, aqlli ob’ektlarning joylashishi tezlik va energiya iste’moli nuqtai nazaridan apparatda yaxshi ishlaydigan shifrlarga e’tiborning ortishiga olib keladi. 2.1-jadvalda ko‘rsatilgan LWC algoritmlari bevosita taqqoslangan, xususan, quyidagi ko‘rsatkichlardan foydalanilgan: kalit o‘lchami, blok o‘lchami, raundlar soni, mantiqiy elementlar ekvivalentlarida (GE) o‘lchangan iste’mol qilingan maydon va kod hajmi (baytlarda). GE uchun keltirilgan qiymatlar apparat ta’minotiga bog‘liq bo‘lsa, kod hajmi esa dasturiy ta’minotga tegishli.

2.1-jadval

Turli LWC algoritmlarining qiyosiy tahlili

	Cipher	Key size (bits)	Block size (bits)	Rounds (hardware impl.)	GE (software impl.)	Code size (bytes)
Software ciphers	AES	128	128	10	3400 [127, 128]	2606
	TEA	128	64	32	3490 [129]	1140
					3758 [a] [130]	
	$SEA_{96,8}$	96	8	$\geq 3n/4$	3925 [b] [130]	2132
					2547 [131]	
Hardware ciphers	PRESENT	80	64	32	1570 [123]	936
	HIGHT	128	64	32	3048 [125]	5672

a) Round-based implementation with datapath of size n
b) Serialized implementation with datapath of size b.

2.3. Yengil ochiq kalitli kriptografik algoritmlar

Ochiq kalitli (assimetrik) kriptografiya ochiq kalit va shaxsiy kalitdan foydalanishni talab qiladi. Ochiq kalitlar tugun(node)ning identifikatori bilan ularni sertifikatni tekshirish uchun so‘raladigan sertifikatlashtirish organi tomonidan imzolangan ochiq sertifikatga kiritish orqali bog‘lanishi mumkin. Ochiq kalitli kriptografiya ochiq kalitli infratuzilmani o‘rnatish uchun yetarli harakatni talab qiladi. Bundan tashqari, assimetrik kriptografiya yuqori ishlov berish va katta hajmli kalitlarni talab qiladi (RSA uchun kamida 1024 bit). Muqobil ochiq kalitli kriptografik sxemalar, masalan, elliptik egri chiziqli kriptografiya, RSA kalitlari bilan bir xil xavfsizlikka erishish uchun kamroq uzunlikdagi kalitlardan foydalanishni talab qiladi. Biroq, shu sababli, qayta ishlash tezligi, hisoblash harakatlari va uzatiladigan xabarlar hajmi bo‘yicha simmetrik kriptografiya afzalroqdir. Ochiq kalitli shifrlar odatda simmetrik kalitlarni almashinish uchun ishlatiladi.

RSA algoritmi

Rivest, **S**hamir va **A**dleman (RSA) algoritmi eng mashhur va keng qo‘llaniladigan ochiq kalitli shifrlash sxemasidir. U N butun son moduli bo‘yicha chekli maydonda darajaga ko‘tarilishga asoslanadi. N moduli va bir juft ochiq va shaxsiy kalitlar (e, d) berilgan bo‘lsin. m xabarining shifrlanishi $c = m^e mod\ N$ tenglik bilan, deshifrlanishi esa $m = c^d mod\ N$. Ochiq-shaxsiy kalit juftligini yaratish quyidagi bosqichlardan iborat:

1) p va q deb belgilangan ikkita katta tub sonni tanlanadi, shunda $p \neq q$ bo‘lsin.

2) $n = p \cdot q$ hisoblanadi.

3) Eylerning totient funksiyasi $\varphi(n) = (p - 1) \cdot (q - 1)$ ni hisoblanadi.

4) $1 < e < \varphi(n)$ va $EKUB(e, \varphi(n)) = 1$ bo‘ladigan butun e soni tanlanadi.

5) $d = e^{-1} mod\ \varphi(n)$ ni hisoblanadi.

Juft (n, e) ochiq kalit, d esa shaxsiy kalit.

RSA algoritmining xavfsizligi katta butun sonlarni faktorizatsiyalashning qiyinligi muammosiga bog‘liq. Qabul qilinadigan xavfsizlik darajasiga erishish

uchun n kamida 1024 bit uzunlikda bo‘lishi kerak, shuning uchun p va q va natijada $\varphi(n)$ ni olish mumkin emas, bu esa (e, d) juftligini himoya qiladi. RSA cheklangan qurilmalarda qo‘llash uchun mos emas, chunki ko‘p sonli qurilmalarda ishlash zarurati va etarli xavfsizlikka erishish uchun katta o‘lchamli kalitlar talab qilinadi. Bundan tashqari, kalitlarni yaratish ham, shifrlash/deshifrlash ham energiya sarfini oshiradigan jarayonlar hisoblanadi.

Elliptik egri chiziqli kriptografiya

Elliptik egri chiziqli kriptografiya (Elliptic curve cryptography, ECC) - bu cheklangan maydonlar ustidagi elliptik egri chiziqlarning algebraik tuzilishiga asoslangan ochiq kalitli kriptografiyaga yondashuvidir. RSA cheklangan maydonlarda eksponentsiyaga asoslangan bo‘lsa, ECC elliptik egri chiziqlardagi nuqtalarni ko‘paytirishga bog‘liq. Cheklangan K maydoni ustidagi (xarakteristikasi 2 va 3 ga teng bo‘lmagan) elliptik egri E quyidagicha aniqlanadi:

$$E(K) : y^2 = x^3 + ax + b, \text{ bu yerda, } a, b \in K$$

$P = (x, y) \in E(K)$ nuqtalar abel guruhini tashkil qiladi, shuning uchun nuqta qo‘shish va skalyarga nuqtani ko‘paytirish mumkin.

ECC birinchi avlod ochiq kalitlar texnikasi RSA va Diffie-Hellmanga qaraganda yuqori xavfsizlik va yaxshi ishlashni ta’minlaydi. Bundan tashqari, ECC o‘rnatilgan muhitlar uchun eng qiziqarli ochiq kalitli kriptografik oiladir, chunki u 2.2-jadvalda ko‘rsatilganidek, ancha qisqaroq kalitlar bilan RSA bilan bir xil xavfsizlik darajasiga erisha oladi va eksponentsiyadan ko‘ra qo‘shish va ko‘paytirish kabi hisoblash jihatidan engilroq amallarga asoslanadi.

2.2-jadval

Simmetrik shifrlar, ECC va RSA uchun xavfsizlik darajalarini taqqoslash (tavsiya etilgan NIST kalit o‘lchamlari)

Symmetric key size (bits)	80	112	128	192	256
ECC key size (bits)	160	224	256	384	512
RSA key size (bits)	1024	2048	3072	7680	15360

ECC tijoriy jihatdan qabul qilingan va Amerika Milliy Standartlar Instituti (American National Standards Institute, ANSI), Elektr va elektronika muhandislari instituti (Institute of Electrical and Electronics Engineers, IEEE), Xalqaro Standartlashtirish Tashkiloti (International Organization for Standardization, ISO), Samarali Kriptografiya Standartlari Guruhi (Standards for Efficient Cryptography Group, SECG) va Milliy standartlar va texnologiyalar instituti (National Institute of Standards and Technology, NIST) kabi standartlar institutlari tomonidan qabul qilingan.

Cheklangan qurilmalar uchun yengil vaznli apparat ko‘rinishdagi ECC protsessorini joriy qilish tobora ortib bormoqda. Qisqa muddatli xavfsizlik uchun 113 bitli binar maydon va o‘rta muddatli xavfsizlik uchun 193 bitli binar maydon bilan ECC uchun kam mantiqiy element talab qiluvchi apparat ko‘rinishlar ishlab chiqilgan. Tub maydon o‘rniga ikkilik maydonni tanlash mos keladigan tashishsiz

arifmetika bilan bog‘liq bo‘lib, u apparat ko‘rinishida amalga oshirish uchun mos keladi. Boshqa ECC apparat ko‘rinishdagi versiyalarga qaragada, kamroq GE talab etadi va tezroq bajarilishni namoyon etadi.

Ochiq kalitli kriptografik algoritmlarning unumdorligini taqqoslash

Bu yerda RSA va ECC ochiq kalit algoritmlarini, masalan, TinyECC va Wiselibni, cheklangan qurilmalarda (masalan, 8-bitli Arduino Uno platasi) olingan mezonlarga nisbatan amalga oshirish samaradorligi ko‘rib chiqilgan. 2.4-jadvalda RSA ochiq kalitli shifrlashning amalga oshirish natijalari, agar maxfiy kalit SRAM yoki ROMda saqlangan bo‘lsa, ko‘rsatilgan. 2.5-jadvalda TinyECC va Wiselib ilovalarida ECDSA imzo algoritmlarining ishlashi taqqoslanadi. ROM bo‘yicha taqqoslash 2.3-jadvalda keltirilgan.

2.5-jadval

Ochiq kalitli shifrlash kutubxonasi ROM hajmi

Library	AvrCryptolib	Wiselib	TinyECC	Relic-toolkit
ROM footprint (kB)	3.6	16	18	29

2.6-jadval

RSA shaxsiy kalit bilan ishlash samaradorligi

Key length (bits)	Execution time (ms)		Memory footprint (bytes)	
	Key in SRAM	Key in ROM	Key in SRAM	Key in ROM
64	66	70	40	32
128	124	459	80	64
512	25089	27348	320	256
1024	109666	218367	640	512
2048	1587559	1740267	1280	104

2.7-jadval

ECDSA imzo ishlashi: TinyECC va Wiselib ilovalari

Curve parameters	Execution time (ms)		Memory footprint (bytes)		Comparable RSA key length
	TinyECC	Wiselib	TinyECC	Wiselib	
128r1	1858	10774	776	732	704
128r2	2002	10615	776	732	704
160k1	2228	20164	892	842	1024
160r1	2250	20231	892	842	1024
160r2	2467	20231	892	842	1024
192k1	3425	34486	1008	952	1536
192r1	3578	34558	1008	952	1536

Engil vaznli kriptografik xesh funksiyalar

MD5 va SHA-1 kabi kriptografik xesh funksiyalari kriptografiyadan foydalanadigan har qanday protokolning muhim qismidir. Xesh funksiyalari xabarlar yaxlitligini tekshirish, raqamli imzolar va xesh qiymatlari kabi turli maqsadlarda ishlatiladi. Kriptografik xesh-funksiyalar ideal holda:

• hisoblash jihatidan arzon;

• xesh qiymatdan ma'lumotni qaytarishga (pre-image) chidamli: xesh h berilgan bo'lsa, $h = hash(m)$ bo'ladigan m xabarini olish uchun xesh funksiyasini o'zgartirish qiyin bo'lishi kerak;

• 2 tartibli pre-imagega chidamli: m_1 xabari berilgan bo'lsa, $hash(m_1) = hash(m_2)$ shartni qanoatlantiruvchi boshqa m_2 xabarini topish qiyin bo'lishi kerak;

• kolliziyaga chidamli: $m_1 \neq m_2$ bo'lgan ikkita m_1 va m_2 xabarlarni topish qiyin bo'lishi kerak, bu yerda, $hash(m_1) = hash(m_2)$.

Umuman olganda, n-bitli chiqishga ega xesh funksiya uchun pre-image va ikkinchi tartibli pre-imagega qarshilik 2^n operatsiyani talab qilishi, kolliziyaga bardoshlilik esa $2^{n/2}$ operatsiyani talab qilishi lozim. Standart kriptografik xesh-funksiyalarni loyihalash apparat samaradorligiga e'tibor qaratmasada, GE nuqtai nazaridan va energiya sarfini minimallashtirish uchun resurslari cheklangan qurilmalarda foydalanish uchun yengil vaznli kriptografik xesh funksiyalari kerak bo'ladi. Quyida ba'zi yengil vaznli xesh funksiyalar bilan tanishib chiqiladi.

DM-PRESENT va H-PRESENT

Bogdanov va boshqalar PRESENT blok shifriga asoslangan DM-PRESENT va H-PRESENT, ikkita yengil vaznli xesh funksiyalarini taklif qilishgan. DM-PRESENT 64-bitli xesh-funksiya bo'lib, ikkita versiyada mavjud: ya'ni qaysi shifr (PRESENT-80 yoki PRESENT-128) ishlatilishiga qarab DM-PRESENT-80 va DM-PRESENT-128. H-PRESENT (ya'ni H-PRESENT-128)-bu PRESENT-128 blok shifriga asoslangan 128 bitli xesh-funksiya. Mualliflar o'z ishlarida xavfsizlik darajasini oshirish uchun PRESENT blok shifriga asoslangan uzunroq xesh qiymatli xesh-funksiyalarni qurish muammosini ham ko'rib chiqqan.

PHOTON

PHOTON - bu cheklangan qurilmalar uchun mo'ljallangan kriptografik xesh-funktsiyalarning apparatga yo'naltirilgan oilasi. PHOTON domenni kengaytirish algoritmi sifatida shimgichga (sponge) o'xshash konstruktsiyadan va ichki kalitsiz almashtirish sifatida AESga o'xshash akslantirishdan foydalanadi. PHOTON namunasi uning chiqish hajmi ($64 \leq n \leq 256$), kirish tezligi r va chiqish tezligi r' ($PHOTON - n / r / r'$) bilan aniqlanadi. Shimgich funktsiyasi freymworkidan foydalanish ichki xotiradan foydalanishni past darajada saqlashga qaratilgan. Kichkina xabarlarni xeshlashda tezlikni oshirish uchun freymwork kengaytirilgan va bu odatda shimgich funksiyasi freymworkida samarasiz.

SPONGENT

SPONGENT - bu 88, 128, 160, 224 va 256 bitli chiqishlarga ega yengil vaznli xesh-funksiyalar oilasi. SPONGENT PRESENT tipidagi almashtirishga ega shimgich konstruktsiyasiga asoslangan. SPONGENT nomlanishi chiqish hajmi n, tezligi r va sig'im c ($SPONGENT - n / c / r$) bilan aniqlanadi. Kenglik (width) sifatida belgilangan ichki holatning o'lchami $b = r + c \geq n$. ASIC apparatidagi

ilovalar mos ravishda 738, 1060, 1329, 1728 va 1950 GE ni talab qiladi, bu esa uni apparatdagi eng kichik maydonga ega xesh funksiyasiga aylantiradi. 88-bitli xesh o‘lchami faqat pre-image muammosiga qarshilikka erishish uchun ishlatiladi.

QUARK

QUARK xesh oilasi uchta variantda mavjud: U-QUARK, D-QUARK va S-QUARK, mos ravishda 136, 176 va 256 bit xesh o‘lchamlariga ega. QUARK, xuddi PHOTON va SPONGENT kabi, shimgich konstruktsiyasiga asoslangan. QUARK xesh oilasi apparat ko‘rinishda amalga oshirish uchun optimallashtirilgan va mualliflar ta’kidlaganidek, dasturiy ta’minotni amalga oshirish o‘rniga boshqa loyihalarga tayanishi kerak. QUARK PHOTON va SPONGENTga qaraganda kattaroq xotira sohasini talab etadi, lekin SPONGENTga qaraganda yuqori o‘tkazuvchanlikni va PHOTONga qaraganda yaxshiroq xavfsizlikni ko‘rsatadi.

Keccak

Keccak - shimgich funktsiyalar oilasi. Keccak shimgichli konstruktsiyadan foydalanadi, unda xabar bloklari holatning boshlang‘ich bitlariga XORlanadi, so‘ngra ular teskari o‘zgartiriladi. Keccakda qo‘llanilgan versiyada holat 64 bitli so‘zlarning 5 × 5 massividan iborat: jami 1600 bit. Keccak o‘zgaruvchan chiqish uzunligini ta’minlaydi. Keccak NIST tomonidan 2012-yil 2-oktabrda SHA-3 tanlovi g‘olibi sifatida tanlandi. O‘shandan beri u SHA-3 deb nomlanadi.

SQUASH

SQUASH (SQUare-hASH) RFID teglari kabi cheklangan qurilmalarda savol-javob tizimidagi MAC ilovalarida ishlash uchun mo‘ljallangan. SQUASH butunlay deterministik va shuning uchun u tasodifiy qiymatlar uchun ichki manbani talab qilmaydi. SQUASH 64-bitli pre-imagega nisbatan qarshilikni taqdim etadi. SQUASH kolliziyaga chidamli emas. Biroq, u RFID autentifikatsiya protokollariga mo‘ljallangani va bu yerda kolliziyaga bardoshli bo‘lishi talab etilmagani bois muammo emas. Agar kolliziyaga bardoshlilik talab etilsa, masalan, raqamli imzolar uchun, SQUASH mos kelmaydi va boshqa xesh-funksiyalardan foydalanish talab etiladi.

2.4. Gomomorfik shifrlash usullari

Gamomorfik shifrlash – shifrlash ko‘rinish bo‘lib, shifrmatnlar ustida hisoblash imkonini beradi, ya’ni ochiq matn ko‘rinishda bo‘lgan ma’lumotlar ustida olib borilgan biror amal natijasi shifrmatnlar ustida olib borilgan boshqa biror amal natijasi bilan bir xil bo‘ladi.

Bulutli hisoblash tizimlarida yuborilgan shifr matnlarni deshifrlamasdan ular ustida amal bajarish ham vaqt ham xarajat nuqtai – nazaridan maqul usuldir. Bu esa gamomorfik shifrlash tizimlaridan foydalanish yuqori samara berishini anglatadi.

Gamomorfik shifrlash tashqi manbalarni saqlash va hisoblash uchun maxfiylikni saqlash uchun ishlatilishi mumkin. Bu ma’lumotlarni shifrlash va qayta ishlash uchun tijorat bulutli muhitga uzatish, barchasini shifrlashga imkon beradi. Sog‘liqni saqlash kabi yuqori darajada boshqariladigan sohalarda, ma’lumot almashishni taqiqlovchi maxfiylik to‘siqlarini olib tashlash orqali yangi xizmatlarni yoqish uchun gamomorfik shifrlashdan foydalanish mumkin. Masalan, sog‘liqni saqlash sohasidagi bashoratli tahlillarni tibbiy ma’lumotlarning maxfiyligi bilan bog‘liq muammolar tufayli qo‘llash qiyin, ammo agar bashoratli tahlil xizmati

provayder shifrlangan ma’lumot asosida ishlasa, ushbu maxfiylik muammolari kamayadi.

Gamomorfik shifrlash - bu shifrlangan ma’lumotni maxfiy kalitdan foydalanmasdan hisoblash uchun qo‘shimcha baholash imkoniyati bo‘lgan *shifrlash* shakli. Bunday hisoblash natijasi shifrlangan bo‘lib qolmoqda. Gamomorfik shifrlash *simmetrik kalitli* yoki *ochiq kalitli kriptografiyan*ing kengaytmasi sifatida ko‘rib chiqilishi mumkin. Gamomorfiya algebradagi gamomorfizmga ishora qiladi: *shifrlash* va *deshifrlash* funksiyalari oddiy matn va shifrlangan matnlar orasidagi gamomorfizm deb o‘ylash mumkin.

Gamomorfik shifrlash bir necha turdagi shifrlash sxemalarini o‘z ichiga oladi, ular shifrlangan ma’lumotlarga nisbatan har xil hisoblashlarni bajarishi mumkin. Gamomorfik shifrlashning ba’zi keng tarqalgan turlari *qisman gamomorfik* (*partially homomorphic*), *biroz gamomorfik (somewhat homomorphic)*, *darajalangan to‘liq gamomorfik (leveled fully homomorphic)* va *to‘liq gamomorfik (fully homomorphic)* shifrlashdir. Hisoblashlar ham mantiqiy, ham arifmetik aylanishlar shaklida berilgan. *Qisman gamomorfik* shifrlash faqat bitta turdagi amaldan, masalan, qo‘shish yoki ko‘paytirishdan iborat bo‘lgan davrda baholashni qo‘llab-quvvatlovchi sxemalarni o‘z ichiga oladi. *Biroz gamomorfik* shifrlash sxemalari ikkita turdagi amallarni baholashi mumkin. *Darajalangan to‘liq* gamomorfik shifrlash chegaralangan (oldindan aniqlangan) amallarni qo‘llab quvvatlaydi. *To‘liq* gamomorfik shifrlash barcha amallarni uchun qo‘llash imkonin beradi va gamomorfik shifrlashning eng amaliy jihatdan to‘liq joriy qilish imkoniyatiga ega ko‘rinishidir.

Qisman gamomorfik shifrlash. Biror ochiq ma’lumot m ni shifrlash funksiyasi $\varepsilon(m)$ belgilanishlaridan foydalanib quyidagilarni yozish mumkin.

RSA algoritmida. Agar RSA algoritmida ochiq matn *x* ni ochiq kalit *e* bilan shifrlash funksiyasi $\varepsilon(x) = m^e mod m$ ga teng bo‘lsa, u holda gamomorfik xususiyat quyidagiga teng bo‘ladi:

$$\varepsilon(x_1) \cdot \varepsilon(x_2) = x_1^e x_2^e mod m = (x_1 x_2)^e mod m = \varepsilon(x_1 \cdot x_2)$$

El – Gamal algoritmida. Ushbu kriptotizimda siklik guruh G uning tartibi q va asos g bo‘lganda, ochiq kalit (G, q, g, h) ga teng. Bu yerda, $h = g^x$ va x esa maxfiy kalit. Bu holda m ma’lumotni shifrlash funksiyasi $r \in \{0, \dots, q-1\}$ lar uchun $\varepsilon(m) = (g^r, m \cdot h^r)$ ga teng. Ushbu algoritm uchun gamomorfik xususiyat quyidagiga teng bo‘ladi:

$$\varepsilon(m_1) \cdot \varepsilon(m_2) = (g^{r_1}, m_1 \cdot h^{r_1})(g^{r_2}, m_2 \cdot h^{r_2}) = (g^{r_1+r_2}, (m_1 \cdot m_2)h^{r_1+r_2}) = \varepsilon(m_1 \cdot m_2).$$

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

$$\varepsilon(b_1) \cdot \varepsilon(b_2) = (x^{b_1} r_1^2 x^{b_2} r_2^2) mod m = (x^{b_1+b_2}(r_1 r_2)^2) mod m = \varepsilon(b_1 \oplus b_2).$$

Benaloh algorimtida. Ushbu algoritmda, agar ochiq kalit modul *m* ga, asos *g*

ga va blok o‘lchami s ga teng bo‘lsa, berilgan $r \in \{0, \dots, m-1\}$ sonlari uchun x xabarni shifrlash funksiyasi $\varepsilon(x) = g^x r^c mod\, m$ ga teng bo‘ladi. Bu holda gamomorfik xususiyat quyidagiga teng bo‘ladi:

$$\varepsilon(x_1) \cdot \varepsilon(x_2) mod\, m = (g^{x_1} r_1^c)(g^{x_2} r_2^c) mod m = g^{x_1+x_2}(r_1 r_2)^c$$
$$= \varepsilon(x_1 + x_2 mod m)$$

Pailler algoritmida. Ushbu algoritmda, ochiq kalit modul m va asos g dan iborat bo‘lsa, berilgan $r \in \{0, \dots, m-1\}$ sonlari uchun x xabarni shifrlash funksiyasi $\varepsilon(x) = g^x r^m mod m^2$ ga teng bo‘ladi. U holda gamomorfik xususiyat quyidagiga teng bo‘ladi:

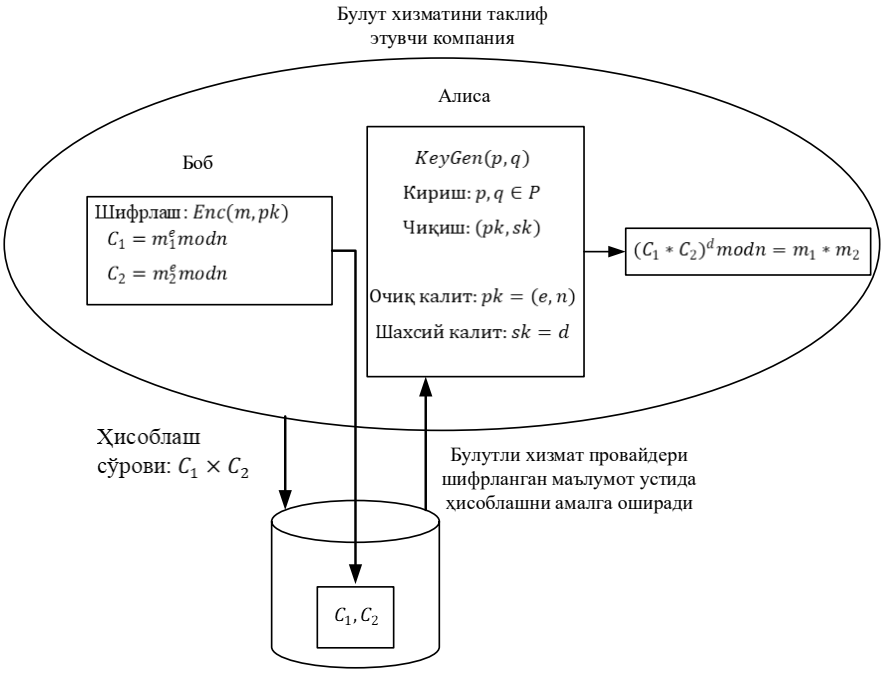
$$\varepsilon(x_1) \cdot \varepsilon(x_2) = (g^{x_1} r_1^m)(g^{x_2} r_2^m) mod m^2 = g^{x_1+x_2}(r_1 r_2)^m mod m^2 = \varepsilon(x_1 + x_2)$$

Multiplikativ gamomorfik shifrlash (RSA kriptotizimi asosida). Agar p va q sonlari tub bo‘lsa, u holda $n = p * q$ bo‘lsin. $e * d \equiv 1(mod\phi(n))$ tenglikni qanoatlantiruvchi e va d sonlari aniqlanadi. $n\ va\ e$ ochiq kalit hisoblansa, d shaxsiy kalit hisoblanadi. Mazkur holda RSA algoritmida shifrlash tengligi $C = M^e mod n$ ga teng bo‘lsa, deshirflash tengligi $M = C^d mod n$ ga teng bo‘ladi.

Gamomorflik: agar x_1 va x_2 ochiq matnlar bo‘lsa, u holda:

$$\varepsilon(x_1) \cdot \varepsilon(x_2) = x_1^e x_2^e mod m = (x_1 x_2)^e mod m = \varepsilon(x_1 \cdot x_2)$$

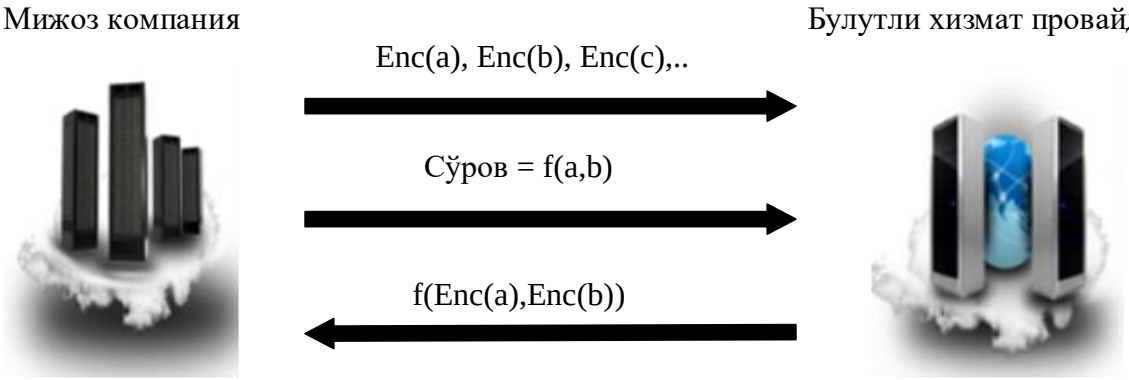
Bulutli hisoblash tizimida amalga oshirilgan multiplikativ gamomorfik shifrlashning umumiy ko‘rinish 2.7-rasmda keltirilgan.



2.7-rasm. Multiplikativ gamomorfik shifrlashni bulutli hisoblashda qo‘llash

Keltirilgan gamomorfik shirflash faqat ko‘paytiruv amalini qo‘llaydi. Bulutda barcha turdagi hisoblashlarni amalga oshirish uchun esa to‘liq gamamorfik shifrlashni amalga oshirish talab qilinadi. 2009-yilda IBM tashkiloti Gentry deb nomlanuvchi to‘liq gamomorfik shifrlash tizimini taklif qildi. Bu usul o‘zgaruvchan sondagi qo‘shish va ko‘paytirishni amalga oshiradi va shuning uchun shirflangan matnda istalgan turdagi shifrlash amalga oshirish imkoniyatiga ega. Bulutli

hisoblash tizimlari xavfsizligida to‘liq gamomorfik shifrlash imkoniyatiga ega dasturiy vositalar juda muhim bo‘lib, ular maxfiy ma’lumotlarni turli uzellarda oshkor bo‘lmasligini oldini oladi. Umumiy holda bulutli hisoblash tizimlarida to‘liq gamomorfik shifrlashni qo‘llashning umumiy ko‘rinishi 2.8-rasmda keltirilgan.



2.8-rasm. To‘liq gamomorfik shifrlashning bulutli hisoblashda tatbig‘i

Umumiy holda keng tarqalgan gamomorfik shirflash algoritlarining qiyosiy tahlili va xususiyatlari 2.8-jadvalda keltirilgan.

2.8-jadval

Gamomorfik shirflash algoritlarining qiyosiy tahlili va xususiyatlari

Xususiyatlar	**Gamomorfik shifrlash tizimlari**					
	RSA	**Paillier**	**El-Gamal**	**Goldwasser-Micali**	**Boneh-Goh-Nissim**	**Gentry**
Platforma	Bulutli hisoblash					
Gamomorfik shifrlash turi	Ko‘paytiruv	Qo‘shuv	Ko‘paytiruv	Qo‘shuv, biroq, faqat bir bitni shifrlaydi	Cheklanmagan sondagi qo‘shuv, biroq, bir ko‘paytiruv	To‘liq
Ma’lumot shaxsiyligi	Aloqa va saqlash jarayonlarida ta’minlanadi					
... ga xavfsizlik qo‘llaniladi	Bulutli xizmat provayderi					
Kalitlar ... tomonidan foydalaniladi	Mijozlar (shifrlash va deshifrlash uchun turli kalitlar foydalaniladi)					

2.5. Yengil kriptografik protokol: DTLS

Datagram Transport Layer Security (DTLS) - bu datagramga asoslangan bog‘lanishlar uchun maxfiylik, yaxlitlik va autentifikatsiyani ta’minlash uchun mo‘ljallangan xavfsizlik protokoli. Bu asosan HTTP-larda tez-tez ishlatiladigan TLS (Transport Layer Security) protokolining User Datagram Protocol (UDP) uchun moslashtirilgan variantidir. DTLS IoT muhitlari uchun juda muhim bo‘lib, bu yerda ko‘plab cheklangan qurilmalar yengil, kam quvvatli va past kechikishli aloqa uchun UDP ga tayanadi.

DTLS IoT ilovalarida CoAP (Constrained Application Protocol) kabi protokollarni himoya qilish uchun keng qo‘llaniladi, bu qurilmalar o‘rtasida uzatiladigan ma’lumotlarni hatto UDP kabi ishonchsiz va ulanishsiz tarmoqlar orqali ham tinglash, buzish va qalbakilashtirishdan himoyalanganligini ta’minlaydi.

IoTda DTLS ning asosiy xususiyatlari:

1. Yengil vaznli va UDPga asoslangan: DTLS UDP orqali ishlaydi, bu odatda TCP ga qaraganda kam resurs talab etadi. Ushbu loyiha DTLS quvvat, ishlov berish va tarmoq imkoniyati cheklangan IoT ilovalarida samarali ishlashiga imkon beradi.

2. Ulanishsiz xavfsizlik: DTLS UDP orqali nuqtadan nuqtagacha xavfsizlikni ta'minlaydi, u holatsiz va ulanishsizdir, ya'ni DTLS uzluksiz ulanishga tayanmaydi, shuning uchun uni tarmoqqa vaqti-vaqti bilan ulanadigan qurilmalar uchun mos deyish mumkin.

3. Paket yo'qotilishi va qayta tartiblanishiga chidamlilik: DTLS paketlarni yo'qotish, tartibni o'zgartirish va xabarlarni takrorlash kabi UDP'dagi umumiy muammolarni hal qilish uchun mo'ljallangan. Xabarlar tartibini kuzatish mexanizmlarini o'z ichiga olgan holda, DTLS tartibsiz yoki takroriy xabarlarni aniqlay oladi va qayta ishlaydi, bu ayniqsa xalaqitli simsiz muhitda ishlaydigan IoT qurilmalari uchun foydalidir.

4. Seansni qayta boshlash va keshlash: DTLS seansni qayta boshlashni qo'llab-quvvatlaydi, bu IoT qurilmalariga avval o'rnatilgan seanslarni to'liq qo'l siqish jarayonisiz (Handshake protokolini ishlatmasdan) davom ettirish imkonini beradi. Bu xususiyat hisoblash resurslari va vaqtni tejaydi, bu cheklangan qurilmalar uchun ideal holatdir.

5. O'zaro autentifikatsiya: DTLS turli autentifikatsiya rejimlarini qo'llab-quvvatlaydi, jumladan:

- *Oldindan taqsimlangan kalit (Pre-shared Key, PSK):* Ikkala qurilma ham simmetrik kalitni oldindan taqsimlaydi. PSK rejimi samaradorligi tufayli kam quvvatli qurilmalar uchun mos keladi.

- *Xom (raw) ochiq kalit:* Ochiq kalitlar sertifikatlarsiz almashtiriladi, bu to'liq ochiq kalit infratuzilmasi (Public Key Infrastructure, PKI) bilan solishtirganda qo'shimcha xarajatlarni kamaytirib, haqiqiylikni ta'minlaydi.

- *Sertifikatlar:* Qurilmalar raqamli sertifikatlar yordamida bir-birini autentifikatsiyalaydi, kuchli xavfsizlik darajasini ta'minlaydi, lekin ko'proq resurs talab qiladi.

DTLS qo'l siqish (Handshake) jarayoni

TLSga o'xshash DTLS qo'l siqish jarayoni umumiy shifrlash kalitlari bilan xavfsiz seansni o'rnatish uchun mijoz va server o'rtasida ko'p bosqichli kelishuvlardan iboratdir. Bu quyidagicha ishlaydi:

1. ClientHello: Mijoz kriptografik parametrlarni taklif qiluvchi ClientHello xabari bilan qo'l siqishni boshlaydi (masalan, qo'llab-quvvatlanadigan shifrlar to'plami va seans identifikatori).

2. ServerHello: Server parametrlarni tasdiqlab, mos shifrlash algoritmlarini tanlab, ServerHello bilan javob beradi.

3. Sertifikat almashinuvi: Agar sertifikatlar ishlatilsa, server o'z sertifikatini mijoz autentifikatsiyasi uchun yuboradi. O'zaro autentifikatsiya qilish uchun mijoz o'z sertifikatini ham yuboradi.

4. Kalit almashinuvi: Mijoz va server simmetrik kalitlarni yaratish yoki kalit kelishuvi uchun assimetrik kriptografiyadan foydalanish orqali kalit ma'lumotlarini almashadilar.

5. Tugallangan xabarlar: Mijoz ham, server ham almashilgan xabarlar xeshlarini o‘z ichiga olgan “Bajarildi” xabarlarini jo‘natadi, bu esa har biriga qo‘l siqish yaxlitligini tekshirish imkonini beradi.

6. Seans o‘rnatildi: Agar barcha tekshiruvlar o‘tsa, xavfsiz seans o‘rnatiladi. Mijoz va server endi simmetrik shifrlash yordamida xavfsiz muloqot qilishlari mumkin.

DTLS UDP orqali qo‘l siqish ishonchliligini oshirish uchun qo‘l siqish xabarlarini qayta uzatish kabi mexanizmlarni taqdim etadi. Bu jarayon ulanish ishonchsiz bo‘lishi mumkin bo‘lgan IoT qurilmalari uchun juda muhimdir, chunki u ikkala qurilmaning ham seansni muvaffaqiyatli o‘rnatishini ta’minlaydi.

Resurs cheklangan IoT qurilmalaridagi DTLS:

IoT qurilmalari ko‘pincha protsessor, xotira, quvvat va tarmoq o‘tkazish qobiliyati jihatidan cheklangan. DTLS bunday muhitda uni amalga oshirish mumkin bo‘lgan moslashtirish va optimallashtirishlarga ega:

1. Kam quvvat sarflaydigan qurilmalar uchun DTLS 1.2: DTLS 1.2 an’anaviy RSA’dan pastroq hisoblash narxida kuchli xavfsizlikni ta’minlovchi elliptik egri chiziq kriptografiyasi (ECC) kabi yanada samarali kriptografik variantlarni taklif etadi. Cheklangan qurilmalar uchun ECC asosidagi kalit almashinuvi va imzolanishi yaxshi variant hisoblanadi.

2. Sessiyani davom ettirish: Seansni qayta boshlash IoT uchun foydalidir, chunki u qayta ulanishda to‘liq qo‘l siqishni o‘tkazib yuboradi. IoT qurilmalari quvvatni tejash va DTLS seanslarini keyinroq minimal energiya sarfi bilan davom ettirish uchun uxlash (sleep) rejimiga o‘tishi mumkin.

3. Xabarni bo‘laklash va qayta yig‘ish: DTLS katta xabarlarni UDP datagrammalariga mos keladigan kichikroq bo‘laklarga bo‘lish orqali xabarlarni bo‘laklashni qo‘llab-quvvatlaydi. Bu xususiyat 6LoWPAN yoki IEEE 802.15.4 asosidagi tarmoqlar kabi past maksimal uzatish birliklari (maximum transmission units, MTU) bo‘lgan IoT tarmoqlarida foydalidir.

4. Tanlangan xavfsizlik darajalari: IoT ilovasining imkoniyatiga qarab, DTLS qurilmalarga xavfsizlik konfiguratsiyasini sozlash imkonini beradi. Masalan, ba’zi ilovalar samaradorlik uchun PSK dan foydalanishi mumkin, boshqalari esa yuqori darajadagi xavfsizlik talablari sertifikatlardan foydalanishi mumkin.

IoT uchun DTLS xavfsizlik rejimlari

NoSec: Shifrlash yoki autentifikatsiya yo‘q, faqat kelajakda xavfsiz konfiguratsiyalar bilan potentsial muvofiqligi uchun DTLSga tayanadi.

Oldindan almashinilgan umumiy kalit (PSK): mijoz ham, server ham oldindan ma’lum bo‘lgan umumiy kalitga ega. PSK rejimi samarali va cheklangan resurslarga ega IoT qurilmalari uchun mos, lekin joylashtirishdan oldin kalitlarni xavfsiz taqsimlashni talab qiladi.

Xom ochiq kalit: Har bir qurilmada sertifikatsiz umumiy/maxfiy kalitlar juftligi mavjud. Ushbu rejim sertifikatga asoslangan autentifikatsiyadan ko‘ra kamroq manba talablari bilan o‘rtacha xavfsizlikni ta’minlaydi.

Sertifikatga asoslangan autentifikatsiya: Qurilmalar o‘zaro autentifikatsiya uchun X.509 sertifikatlaridan foydalanadi, bu esa yuqoriroq resurslar sarfi evaziga mustahkam xavfsizlikni ta’minlaydi. Bu o‘rtacha va yuqori resurslarga ega yuqori

darajadagi xavfsiz IoT ilovalari uchun javob beradi.

IoT uchun DTLS da xavfsizlik muammolari

Afzalliklariga qaramay, DTLS IoT muhitida ba’zi qiyinchiliklarga ega:

Qayta ishlash xarajatlari: DTLS-ning kriptografik operatsiyalari, ayniqsa sertifikatlar bilan, cheklangan qurilmalarda talab qilinishi mumkin. IoT protokollari DTLS bilan samarali ishlash uchun apparat tezlashuvi yoki optimallashtirilgan kriptografik kutubxonalarni talab qilishi mumkin.

Paketni yo‘qotish va qayta tartiblashga moyillik: DTLS tartibsiz paketlarni ishlasa ham, paketlarni haddan tashqari yo‘qotish yoki qayta tartiblash seanslarni, ayniqsa qo‘l siqish paytida buzishi mumkin. Ishonchli uzatish mexanizmlari (masalan, qayta uzatish intervallari) IoT barqarorligi uchun juda muhimdir.

Quvvat iste’moli: Kriptografik operatsiyalar va qayta uzatishlar kam quvvatli qurilmalarda batareyaning ishlash muddatini qisqartirishi mumkin. CPU va xotiradan foydalanishni kamaytirish uchun DTLS ilovalarini optimallashtirish qo‘l siqishlarini kamaytirish uchun seansni qayta boshlash kabi yordam berishi mumkin.

Kalitlarni boshqarish: IoT-da kriptografik kalitlarni xavfsiz joylashtirish va boshqarish qiyin, ayniqsa yirik tarmoqlar uchun. PSK va Raw Public Key rejimlaridan foydalanish ba’zi murakkabliklardan qochishga yordam beradi. Ammo sertifikatga asoslangan tizimlar yanada ehtiyotkorlik bilan boshqarishni talab qiladi.

O‘zaro muvofiqlik: Turli ishlab chiqaruvchilarning IoT qurilmalari uzluksiz o‘zaro ishlash uchun mos DTLS ilovalariga muhtoj. IETF Lightweight Implementation Guidance (LWIG) ishchi guruhi tomonidan belgilangan standartlashtirilgan profillar cheklangan qurilmalarda muvofiqlikni yaxshilashga yordam beradi.

IoTda DTLS qo‘llanilishi

Aqlli uy: DTLS aqlli uy qurilmalari (masalan, chiroqlar, termostatlar va qulflar) va ularning kontrollerlari o‘rtasidagi aloqani ruxsatsiz foydalanish va tinglashdan himoya qiladi.

Industrial IoT (IIoT): DTLS sanoat sharoitidagi ma’lumotlarning yaxlitligi va maxfiyligini ta’minlaydi, masalan, zavod muhitidagi sensorlar yoki boshqarish mexanizmlarini.

Sog‘liqni saqlash IoT: taqiladigan va masofaviy sog‘liqni saqlash qurilmalari muhim sog‘liqni saqlash ma’lumotlarini himoya qilish uchun DTLS’dan foydalanadi, bu faqat vakolatli tizimlar ma’lumotlardan foydalanishi yoki ularni o‘zgartirishi mumkinligini anglatadi.

Atrof-muhit monitoringi: DTLS atrof-muhit sharoitlarini (masalan, harorat, ifloslanish) kuzatuvchi, masofaviy ma’lumotlarning ishonchliligini ta’minlaydigan taqsimlangan sensorli tarmoqlarda ma’lumotlarni himoya qiladi.

IoTdagi DTLS versiyalari: DTLS 1.2 va DTLS 1.3

Kamaytirilgan kechikish: DTLS 1.3 qo‘l siqish xabarlarini qisqartiradi, ulanishni o‘rnatish vaqtini minimallashtiradi, bu esa intervalgacha IoT aloqasi uchun yaxshidir.

Yaxshilangan xavfsizlik: DTLS 1.3 ba’zi eski, zaif shifrlar to‘plamlarini olib tashlaydi va DTLS 1.2 ga nisbatan xavfsizlikni yaxshilagan.

Kengaytirilgan chidamlilik: DTLS 1.3 paketlarni yo‘qotish va qayta

tartiblashni boshqarish, yo‘qolgan IoT tarmoqlarida ishlashni yaxshilash uchun yaxshiroq mexanizmlarni taqdim etadi.

DTLS UDP-ga asoslangan IoT aloqasi uchun muhim xavfsizlikni ta’minlaydi, kuchli shifrlashni muvozanatlashtiradi, past yuklanish va hatto yo‘qolgan tarmoqlarda ham ishonchli xabarlarni etkazib beradi. TLS-ni ulanishsiz muhitga moslash orqali DTLS IoT-da CoAP kabi protokollarni himoya qilish uchun asos bo‘lib, resurslar cheklangan IoT tarmoqlarining muammolari va o‘ziga xos talablariga javob beradi.

Nazariy savollari:

1. Ananaviy tarmoq va IoT tarmog‘ini protokollar kesimida farqini ayting?
2. TEA algoritmi, uning ishlash tartibi va variantlari haqida ma’lumot bering?
3. SEA algoritmi va uning xususiyatlarini ayting?
4. PRESENT shifri va uning xususiyatlarini ayting?
5. Yengil vaznli ochiq kalitli kriptografik tizimlar haqida ma’lumot bering?
6. Yengil vanzli xesh funksiyalar haqida ma’lumot bering?
7. Gomomorfik shifrlash yondashuvi va uning afzalliklari?
8. DTLS protokoli va uning xususiyatlarini ayting?
9. DTLS va TLS protokollarini o‘zaro farqini ayting?
10. Nima uchun barcha kriptografik mexanizmlarni IoT uchun mos variantlarini ishlab chiqishga katta e’tibor berilmoqda?

Adabiyotlar va Internet resurslar:

1. Cirani S. et al. Internet of things: architectures, protocols and standards. – John Wiley & Sons, 2018.
2. Akbarov D. Y. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet.
3. https://datatracker.ietf.org/doc/html/rfc6347 - Datagram Transport Layer Security Version 1.2

3-ma’ruza. YENGIL VAZNLI KRIPTOGRAFIYA BO‘YICHA NIST KONKURSI (2 соат)

Reja:

3.1. LWC algoritmlarini tanlab olish bo‘yicha o‘tkazilgan konkurslar
3.2. LWC algoritmlarini standartlashtirish
3.3. NIST LWC konkursi va uning natijalari
3.4. NIST LWC konkursi ishtirokchilarining chiziqsiz akslantirishlarining tahlili

Tayanch iboralar: *konkurs, eSTREAM loyihasi, Authenticated Encryption with Associated Data, CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) loyihasi, NIST (National Institute of Standards and Technology) konkursi, ISO/IEC (International Organization of Standardization/ International Electrotechnical Commission) 29192 (Information technology — Security techniques — Lightweight cryptography) seriyali standart.*

3.1. LWC algoritmlarini tanlab olish bo‘yicha o‘tkazilgan konkurslar

Buyumlar Interneti (Internet of Things, IoT) texnologiyalarining jadallik bilan rivojlanishi ushbu sohada axborot xavfsizligini ta’minlash masalasini ham hozirgi kundagi dolzarb masalalardan biriga aylantirdi. Bundan tashqari, IoT qurilmalarining odatiy qurilmalarga nisbatan quvvat, hisoblash va tarmoq imkoniyatlarini cheklangan bo‘lishi, ushbu masalani yechishda yanada murakkablik tug‘diradi. Bu esa, IoT qurilmalari uchun mo‘ljallangan xavfsizlik algoritmlarini, xususan, axborotni kafolatlangan himoyasini ta’minlovchi kriptografik algoritmlarni, tadqiq etish kerakligini ko‘rsatadi. IoT qurilmalarida ishlashga mo‘ljallangan kriptografik algoritmlar *yengil vaznli (lightweight cryptography, LWC)* kriprografik algoritmlar deb atalib, bu ularni sodda va yuqori xavfsiz bo‘lmasligini emas, balki yuqori xavfsizlikni ta’minlash bilan birga kam hisoblash, quvvat va tarmoq resurslarini talab etishini va kichik hisoblash qurilmalarida ham amalga oshirish mumkinligini anglatadi.

IoT qurilmalari uchun hozirgacha ko‘p sonli kriptografik algoritmlar ishlab chiqilgan bo‘lib, ularning ba’zilari o‘tkazilgan konkurslar yoki tanlab olish natijasida davlatlarning milliy standarti yoki xalqaro miqiyosida standart sifatida standartlashtirildi. Ushbu maqolada LWC algoritmlarini tanlab olish bo‘yicha o‘tkazilgan konkurslar va standartlashtirish holati tahlil etiladi.

LWC algoritmlarini tanlab olish bo‘yicha o‘tkazilgan konkurslar. LWC algoritmlarni tanlab olish bo‘yicha ko‘plab konkurslar olib borilgan bo‘lib, ularning muhimlari va tanlov natijalari quyida keltirilgan.

eSTREAM loyihasi. Ushbu loyiha 2004-yilda boshlanib g‘oliblar 2008-yilda aniqlangan. Ushbu loyiha NESSIE loyihasida taklif etilgan kriptografik algoritmlar xavfsiz emas deb topilgandan so‘ng, Yevropa ittifoqi tomonidan yangi kriptografik oqimli shifrlarni tanlab olish maqsadida amalga oshirilgan. Ushbu loyihada 2 kategoriya bo‘yicha algoritmlar qabul qilingan:

1. Dasturiy amalga oshirishga qulay va yuqori o‘tkazuvchan oqimli shifrlar (128-bitli kalit, 64 va 128 bitli boshlang‘ich vektorni (IV) qo‘llab quvvatlashi kerak).

2. Qurilmaga amalga oshirishga qulay va cheklangan imkoniyatli qurilmalarda ishlovchi oqimli shifrlar (80-bitli kalit, 32 va 64 bitli IVni qo‘llab quvvatlashi kerak).

Shuningdek, ushbu ikki kategoriyaga autentifikatsiyalovchi shifrlash (Authenticated Encryption with Associated Data, AEAD) va turli uzunlikdagi (32,64,96 yoki 128 bitli) autentifikatsiya tegiga ega shifrlash algoritmlariga bo‘lingan.

Ushbu loyihada jami **34** ta shifrlash algoritmi taqdim etilgan bo‘lib, yakuniy bosqichda ulardan **7** tasi (1-kategoriya uchun **4** ta: **(1)** HC-128 (HC-256), **(2)** Rabbit, **(3)** Salsa20/12 (Salsa20/8, Salsa20), **(4)** (SOSEMANUK) va 2-kategoriya uchun **3** ta: **(1)** Grain v1**, (2)** MICKEY 2.0**, (3)** Trivium) tanlab olingan.

CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) loyihasi. Ushbu loyiha turli muhitlarda foydalanish uchun AEAD turidagi shifrlash algoritmlarini tanlab olish uchun 2012-2019-yillar oralig‘ida xalqaro kriptologik tadqiqotlar jamiyati tomonidan o‘tkazilgan. Ushbu loyihada algoritmlar 3 ta kategoriyada tanlab olingan:

1. LWC turidagi algoritmlar.
2. Yuqori samaradorlikka ega algoritmlar.
3. Yuqori xavfsizlik darajasini ta’minlovchi algoritmlar (Defence in depth).

Ushbu kategoriyalar uchun 2 tadan algoritmlar tanlab olingan:

1. Ascon, ACORN.
2. AEGIS-128, OCB.
3. Deoxys-II, COLM.

NIST (National Institute of Standards and Technology) konkursi. Ushbu konkurs LWC bo‘yicha AEAD turidagi shifrlash va alohida xeshlash algoritmini tanlab olish va standartlashtirish uchun NIST tomonidan 2015-2023-yillar oralig‘ida o‘tkazilgan. AEAD turidagi shifrlash algoritmi uchun kalit uzunligi kamida 128 bit (agar undan tashqari variantlari ham bo‘lsa, ulardan biri 256 bit bo‘lishi), nonce qiymatning uzunligi kamida 96 bit va autentifikatsiya tegining uzunligi kamida 64 bit bo‘lishi talab etilgan. Xesh funksiya uchun xesh qiymatning uzunligi 256 bitdan kam bo‘lmasligi va eng samarali kriptohujumning murakkabligi kamida 2^{112} ga teng bo‘lishi talab etilgan. Bundan tashqari, algoritmlarni 8,16 va 32-bitli mikroprotsessorlarda amalga oshirish mumkin bo‘lishi talab etilgan.

Konkurs 3 ta bosqichda o‘tkazilgan bo‘lib, birinchi bosqichda 56 ta algoritm qabul qilingan bo‘lsa, yakunda ASCON algoritmi tanlab olingan.

3.2. LWC algoritmlarini standartlashtirish

Yuqorida keltirilgani kabi, olib borilgan konkurslar natijasida bir qancha LWC algoritmlari tanlab olingan. Ular esa keyinchalik xalqaro miqiyosida yoki milliy standart sifatida foydalanilishi mumkin. Ular orasidan standartlashtirilgan LWC algoritlari ham mavjud bo‘lib, ushbu sohada standartlashtirish va tavsiyaviy qo‘llanmalar haqida ma’lumot quyida keltirilgan.

ISO/IEC (International Organization of Standardization/ International Electrotechnical Commission) 29192 (Information technology — Security techniques — Lightweight cryptography) seriyali standart. Ushbu standartlar to‘plami 8 ta qismdan iborat bo‘lib, ular quyidagilar:

1-qism: Umumiy (General), 2012-yil.

2-qism: Blokli shifrlar (Block ciphers), 2019-yil.

3-qism: Oqimli shifrlar (Stream ciphers), 2012-yil.

4-qism: Assimetrik usullar yordamida mexanizmlar (Mechanisms using asymmetric techniques), 2013-yil. 2016-yilda qayta ko‘rib chiqilgan.

5-qism: Xesh funksiyalar (Hash-funktions), 2016-yil.

6-qism: Xabarlarni autentifikatsiyalash kodlari (Message authentication codes, MAC), 2019-yil.

7-qism: Broadcast autentifikatsiya protokollari, 2019-yil.

8-qism: Autentifikatsiyalashli shifrlash (Authenticated encryption), 2022-yil.

Ushbu standartga ko‘ra quyidagi algoritmlar tanlab olingan:

Blokli shifrlar: PRESENT, CLEFIA, SIMON va SPECK (biroq tasdiqlanmagan), LEA.

Oqimli shifrlar: Enocoro, Trivium.

Assimetrik usullar: a) elliptik egri chiziqlardagi diskret logarifmlarga asoslangan bir tomonlama autentifikatsiya mexanizmi; b) bir tomonlama autentifikatsiyalash va seans kalitini o‘rnatish uchun autentifikatsiyalangan yengil vaznli kalit almashinuv (Authenticated lightweight key exchange, ALIKE) mexanizmi; c) identifikatsiyaga asoslangan imzo mexanizmi.

Xesh funksiyalar: Photon, Spongent, Lesamnta-LW.

MAC algoritmlar: LightMAC, Tsudik keymode, Chaskey-12.

Broadcast autentifikatsiya protokollari: Timed Efficient Stream Loss-Tolerant Authentication (TESLA).

AEAD shifrlash: Grain-128A.

CRYPTREC (Cryptography Research and Evaluation Committees) loyihasi. Ushbu loyiha Yaponiya elektron hukumat tizimlarida foydalanilgan kriptografik mexanizmlarning xavfsizligini baholash va monitoringni amalga oshiradi. Ushbu loyiha tomonidan 2017-yil mart oyida e’lon qilingan “Cryptographic Technology Guideline (Lightweight Cryptography)” nomli qo‘llanmada quyidagi algoritmlar tanlab olingan:

Blokli shifrlar: AES, Camellia, CLEFIA, TDES, LED, PRINCE, PRESENT, Piccolo, TWINE, SIMON, SPECK, Midori.

AEAD shifrlash: ACORN, AES-GCM, AES-OTR, Ascon, CLOC, SILC, JAMBU, Ketje, Minalpher, AES-OCB.

3.3. NIST LWC konkursi va uning natijalari

NIST (Milliy Standartlar va Texnologiyalar Instituti) yengil vaznli kriptografiya (Lightweight Cryptography) bo‘yicha standartlashtirish jarayonini 2013-yilda boshlagan. Ushbu jarayon cheklangan resurslarga ega qurilmalar uchun samarali va xavfsiz kriptografik algoritmlarni aniqlash va standartlashtirishni maqsad qilgan.

Konkursning asosiy shartlari:

1. Yengil vaznli qurilmalar uchun optimallashtirish: Algoritmlar cheklangan hisoblash kuchi, xotira va energiya sarfiga ega bo‘lgan qurilmalar (IoT, RFID, tibbiy implantlar va boshqalar) uchun mo‘ljallangan bo‘lishi kerak.

2. Asosiy vazifalar: Algoritmlar Authenticated Encryption with Associated

Data (AEAD) va xeshlash vazifalarini bajarishi kerak edi.

3. Xavfsizlik talablari: Algoritmlar zamonaviy kriptografik hujumlarga, jumladan, differensial va linear kriptoanaliz, qo‘shimcha kanal (side-channel) hujumlariga qarshi mustahkam bo‘lishi talab qilindi.

4. Samaradorlik: Algoritmlar ko‘p platformalarda, shu jumladan, apparat va dasturiy ta’minot muhitida ishlash uchun moslashuvchan bo‘lishi kerak.

5. Tanlov jarayoni: Uch bosqichda amalga oshirildi: birinchi raund (2019), ikkinchi raund (2021), final raundi (2023).

Jarayon bosqichlari:

Birinchi bosqich (2019): NIST 57 ta algoritmni qabul qilib, ulardan 56 tasini birinchi bosqichga tanladi.

Ikkinchi bosqich (2019-2021): Birinchi bosqichdan so‘ng, 32 ta algoritm ikkinchi bosqichga o‘tdi.

Final bosqichi (2021-2023): Ikkinchi bosqich natijasida 10 ta finalchi tanlandi: ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU va Xoodyak.

2023-yil fevral oyida NIST ASCON algoritmini yengil vaznli kriptografiya standarti sifatida tanladi. ASCON samaradorlik, xavfsizlik va cheklangan resurslarga ega qurilmalarda ishlash qobiliyati bilan ajralib turadi.

3.1-jadval

NIST LWC final bosqichi algoritmlarining xususiyatlari

Nomi	Turi	Variantlari	Asos sxema	Holat (bit)	Kalit (bit)	Rejim	Blok uzunligi, rate (bit)	Teg (bit)	Xavfsizligi (bit)
Ascon	Sponge	Ascon-128	Ascon-p	320	128	Duplex	64	128	128
		Ascon-128a	Ascon-p	320	128	Duplex	128	128	128
Elephant	Sponge	Jumbo	Spongent	176	128	Elephant	176	64	127
		Dumbo	Spongent	160	128	Elephant	160	64	112
		Delirium	Keccak	200	128	Elephant	176	128	127
GIST-COFB	Block	GIST-COFB	GIFT-128	192	128	COFB	128	128	128
Grain-128AEAD	Oqimli	Grain-128AEAD	N/A	256	128	N/A	1	64	128
ISAP	Sponge	ISAP-A-128	Ascon-p	320	128	ISAP	64	128	128
		ISAP-K-128	Keccak	400	128	ISAP	144	128	128
		ISAP-K-128A	Keccak	400	128	ISAP	144	128	128
		ISAP-A-128A	Ascon-p	320	128	ISAP	64	128	128
PHOTON-Beetle	Sponge	PHOTON-Beetle-AEAD [128]	PHOTON256	256	128	Beetle	128	256	121
		PHOTON-Beetle-AEAD	PHOTON256	256	128	Beetle	32	256	128
Romulus	Block	Romulus-M	Skinny-128-384	384	128	COFB	128	128	128
		Romulus-N	Skinny-128-384	384	128	COFB	128	128	128
		Romulus-T	Skinny-128-384	384	128	COFB	128	128	128
SPARKLE	Sponge	SCHWAEMM256-128	SPARKLE	384	128	SPARKLE	256	128	120
		SCHWAEMM128-128	SPARKLE	256	128	SPARKLE	128	128	120
		SCHWAEMM192-192	SPARKLE	384	192	SPARKLE	192	192	184
		SCHWAEMM256-256	SPARKLE	512	256	SPARKLE	256	256	248
TinyJambu	Sponge	TinyJambu	TinyJambu	128	128	TinyJambu	32	64	120
Xoodyak	Sponge	Xoodyak	Xoodoo	384	128	Cyclist	352	128	128

3.4. NIST LWC konkursi ishtirokchilarining chiziqsiz akslantirishlarining tahlili

ASCON. ASCON algoritmlar oilasi Ascon-128, Ascon-128a, Ascon-80pq

(kvantga asoslangan kalitlarni qidirishga qarshi) autentifikatsiyalashli shifrlash algoritmlari, Ascon-Hash va Ascon-Xof xeshlash algoritmlaridan iborat. ASCON 320 bitli almashtirish ichki holatiga ega bo‘lib, ham apparat ham dasturiy ko‘rinishda amalga oshirishga qulay. Ushbu algoritm oilasi haqida ma’lumotlar 3.1-jadvalda keltirilgan. ASCON oilasida foydalanilgan p almashtirish akslantirishidagi yagona chiziqsiz funksiya p_S bo‘lib, u 5x5 o‘lchamga ega. S jadvalning ko‘rinishi (Look-Up Table, LUT) 3.2-jadvalda keltirilgan.

3.2-jadval

ASCON S jadvalining LUT ko‘rinishi

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
S(x)	4	b	1f	14	1a	15	9	2	1b	5	8	12	1d	3	6	1c	1e	13	7	e	0	d	11	18	10	c	1	19	16	a	f	17

Elephant. Ushbu simmetrik blokli shifrlash algoritmi almashtirish akslantirishiga asoslangan bo‘lib, xabar autentifikatsiyasi uchun shifrlashdan keyin MAC (Message Authentication Code) sxemasidan foydalanilgan. Ushbu algoritmda foydalanilgan loyihalash sxemasi algoritmni ham apparat ham dasturiy ko‘rinishda parallel hisoblash imkoniyatini beradi.

Elephant oilasining Jumbo va Dumbo versiyalari mos holda Spongent-π[160] va Spongent-π[176] almashtirishiga asoslangan va ularda 3.3-jadval keltirilgan 4x4 jadvaldan foydalanilgan. Delirium versiyasida esa Keccak [200] almashtirishidan foydalanilgan.

3.3-jadval

Elephant oilasining dastlabki ikki algoritmida foydalanilgan S jadvalning LUT ko‘rinishi

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	E	D	B	0	2	1	4	F	7	A	8	5	9	C	3	6

GIFT-COFB. NIST LWC konkursida ishtirok etgan 3 algoritm GIFT-COFB bo‘lib, u GIFT blokli shifriga asoslangan va Combined FeedBack (COFB) rejimida autentifikatsiyalashli shifrlashni qo‘llab-quvvatlaydi. Ushbu algoritm 40 raund davomida 4 ta fazadan (initsializatsiya, uyani o‘rniga qo‘yish, bit o‘rnini almashtirib va 128 bitli raund kalitini qo‘shish) iborat SPN (Substitution-permutation network, SPN) iborat shifrlashni amalga oshiradi. Ushbu algoritmning asosi hisoblangan GIFT-128 algoritmi 3 ta fazadan iborat: SubCells, PermBits, va AddRoundKey. Mazkur algoritmda ham 4x4 o‘lchamli S jadvaldan foydalanilgan bo‘lib, uning LUT ko‘rinishi 3.4-jadvalda keltirilgan.

3.4-jadval

GIFT-128 algoritmi S jadvali

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	1	A	4	C	6	F	3	9	2	D	B	7	5	0	8	E

Grain-128AEAD. Ushbu algoritm NIST LWC konkursida ishtirok etgan kam sonli oqimli shifrlardan biri bo‘lib, u Grain shifriga asoslangan. Ushbu algoritm ikki quruvchi blokdan iborat: (1) chiziqli va chiziqsiz teskari aloqali siljitish registrlaridan (Linear Feedback Shift Register, LFSR, Non-linear Feedback Shift Register, NFSR) tashkil topgan chiqishdan oldingi generator va chiqishdan oldingi funksiya, (2) siljitish registori va akkumulyatordan iborat autentifikatsiya generatori. Ushbu algoritm tuzilishi haqiqiy Grain-128a algoritmiga juda o‘xshash bo‘lsada, AEADni qo‘llab quvvatlashi va kattaroq autentifikatorga mo‘ljallangani bilan farqlanadi. Ushbu algoritmning umumiy xususiyatlari 3.1-jadvalda keltirilgan. Ushbu algoritmda chiziqsiz akslantirish sifatida S jadvaldan foydalanilmagan.

ISAP. Ushbu algoritm Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas va Thomas Unterluggauerlar tomonidan yozilgan yengil blokli shifrlash algoritmi bo‘lib, kichik kod o‘lchamli, quvvat tahlili va buzulish hujumlariga bardoshli qilib loyihalashtirilgan. Ushbu algoritmlar oilasi 4 ta variantdan iborat: Isap-K-128a, Isap-A-128a, Isap-K-128, va Isap-A-128, bo‘lib, ularning barchasi kriptografik hujumlarga nisbatan 128 bit xavfsizlik darajasiga ega sifatida loyihalashtirilgan. Ularning 1 va 3-variantlari Keccak-p [400] almashtirishiga asoslangan bo‘lsa, qolganlari 320-bitli Ascon-p almashtirishidan foydalanadi (Ascon-p almashtirishida foydalanilgan S jadval 3.2-jadvaldagi kabi bir xil).

Photon-Beetle. Ushbu algoritmlar oilasi ham Sponge konstruksiyasiga asoslangan bo‘lib, Zhenzhen Bao, Avik Chakraborti, Nilanjan Datta, Jian Guo, Mridul Nandi, Thomas Peyrin, va Kan Yasudalar tomonidan taqdim etilgan. Ushbu algoritm amalga oshirishdagi kichik resurs talab qilgani bilan alohida ajralib turadi. Ushbu algoritm oilasining asosini P256 almashtirishi ($PHOTON_{256}$) tashkil qilib, ushbu almashtirish AddConstant, SubCells, ShiftRows, va MixColumnSerial bosqichlaridan iborat. Ulardan SubCells bosqichi chiziqsiz akslantirishni amalga oshirib, unda foydalanilgan 4 bitli S jadval 3.5-jadvalda keltirilgan.

3.5-jadval

P256 algoritmi S jadvali

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Romulus. Konkursning ushbu ishtirokchisi yuqorida keltirilgan algoritmlar kabi, Sponge konstruksiyasiga emas balki, ananaviy simmetrik blokli shifrlarni qurish usuli *sozlanuvchan blokli shifr (Tweakable block cipher, TBC)* deb nomlanuvchan yondashuvdan foydalangan bo‘lib, buning uchun SKINNY algoritmidan foydalangan. Ushbu algoritm 64 va 128-bitli blok uzunligini, 128 va 256-bitli kalit uzunligini qo‘llab-quvvatlaydi. Ushbu algoritm oilasi haqidagi batafsil ma’lumotlar 3.1-jadvalda keltirilgan. Ikki turdagi blok uzunligi uchun mos

holda 4 bitli va 8 bitli S jadvallardan foydalangan. Ushbu algoritm oilasining faqat 128 bitli blok uzunligi NIST LWC konkursida taqdim etilgani bois, 8 bitli S jadvalning 16 sanoq tizimidagi ifodasi 3.6-jadvalda keltirilgan.

3.6-jadval

Skinny algoritmi S jadvali

x\y	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**0a**	**0b**	**0c**	**0d**	**0e**	**0f**
00	65	4c	6a	42	4b	63	43	6b	55	75	5a	7a	53	73	5b	7b
01	35	8c	3a	81	89	33	80	3b	95	25	98	2a	90	23	99	2b
02	e5	cc	e8	c1	c9	e0	c0	e9	d5	f5	d8	f8	d0	f0	d9	f9
03	a5	1c	a8	12	1b	a0	13	a9	05	b5	0a	b8	03	b0	0b	b9
04	32	88	3c	85	8d	34	84	3d	91	22	9c	2c	94	24	9d	2d
05	62	4a	6c	45	4d	64	44	6d	52	72	5c	7c	54	74	5d	7d
06	a1	1a	ac	15	1d	a4	14	ad	02	b1	0c	bc	04	b4	0d	bd
07	e1	c8	ec	c5	cd	e4	c4	ed	d1	f1	dc	fc	d4	f4	dd	fd
08	36	8e	38	82	8b	30	83	39	96	26	9a	28	93	20	9b	29
09	66	4e	68	41	49	60	40	69	56	76	58	78	50	70	59	79
0a	a6	1e	aa	11	19	a3	10	ab	06	b6	08	ba	00	b3	09	bb
0b	e6	ce	ea	c2	cb	e3	c3	eb	d6	f6	da	fa	d3	f3	db	fb
0c	31	8a	3e	86	8f	37	87	3f	92	21	9e	2e	97	27	9f	2f
0d	61	48	6e	46	4f	67	47	6f	51	71	5e	7e	57	77	5f	7f
0e	a2	18	ae	16	1f	a7	17	af	01	b2	0e	be	07	b7	0f	bf
0f	e2	ca	ee	c6	cf	e7	c7	ef	d2	f2	de	fe	d7	f7	df	ff

Sparkle. Ushbu algoritm oilasi almashtirishga asoslangan bo‘lib, Schwaemm algoritmi konfidensiyallik, yaxlitlik va autentifikatsiyani amalga oshirsa, Esch xeshlash algoritmi esa kolliziyaga bardoshli xesh funksiya hisoblanadi. Har ikkala algoritm ham Sponge konstruksiyasiga asoslangan bo‘lib, ushbu algoritmning NIST LWC konkursida taqdim etilgan varianlari haqida 3.1-jadvalda ma’lumotlar keltirilgan. Ushbu algoritm oilasi Sparkle almashtirishiga asoslangan bo‘lib, ushbu akslantirish o‘z navbatida ARX simmetrik blokli shifrlarni qurish usuliga asoslangan Sparx shifrlash algoritmidan foydalanadi. Boshqacha aytganda, Sparkle oilasi algoritmlarida chiziqsiz akslantirish sifatida S jadvallar o‘rniga ARX almashtirishdan foydalanilgan.

TinyJambu. Ushbu algoritm JAMBU algoritmining ixchamlashtirilgan ko‘rinishi bo‘lib, JAMBU o‘z navbatida CAESAR konkursining 3-bosqich ishtirokchisi hisoblanadi. TinyJAMBU algoritmi kalitli almashtirishga asoslangan bo‘lib, ushbu algoritmning NIST LWC konkursida taqdim etilgan varianti haqidagi umumiy ma’lumotlar 3.1-jadvalda keltirilgan. Ushbu algoritm 128-bit kalitli almashtirishga asoslangan bo‘lib, bunda kalitlarni kengaytirish talab etilmaydi. Ushbu almashtirishning asosini 128-bitli chiziqsiz teskari aloqali siljitish registori tashkil etadi.

Xoodyak. Xoodyak algoritmi Keccak algoritmini yaratgan olimlar jamoasi tomonidan taqdim etilgan bo‘lib, algoritm asosini Xoodoo almashtirish tashkil etadi. Ushbu almashtirish 5 ta bosqichdan iborat: aralashtirish bosqichi (mixing layer) θ, fazoda siljitish bosqichi (plane shifting) ρ_{west}, raund konstantasini qo‘shish bosqichi (addition of round constants) ι, chiziqsiz akslantirish bosqichi (non-linear layer) χ va yana bir fazoda siljitish bosqichi ρ_{east}. χ akslantirish 3 o‘lchamli holat massivining y tekisligi (8x3) ustida amalga ishiriladigan quyidagi ifodadan iborat: $A_0 \leftarrow A_0 + \overline{A_1} \cdot A_2$, $A_1 \leftarrow A_1 + \overline{A_2} \cdot A_0$, $A_2 \leftarrow A_2 + \overline{A_0} \cdot A_1$.

NIST LWC konkursi 3-raund ishtirokchisi bo‘lgan algoritmlarda foydalanilgan chiziqsiz akslantirishlar haqidagi umumiy ma’lumot 3.7-jadvalda keltirilgan.

3.7-jadval

NIST LWC konkursining 3-raund ishtirokchisi bo‘lgan algoritmlarda foydalanilgan chiziqsiz akslantirishlar

№	Algoritm nomi	Chiziqsiz akslantirish turi	Akslantirish o‘lchami
1.	ASCON	S jadval	5→5 (bit)
2.	Elephant	S jadval, Keccak [200] χ akslantirishi	4→4 (bit), 5x5xw→5x5xw (bit)
3.	GIFT-COFB	S jadval	4→4 (bit)
4.	Grain-128AEAD	NFSR	128 bit
5.	ISAP	S jadval, Keccak [400] χ akslantirishi	5→5 (bit), 5x5xw→5x5xw (bit)
6.	Photon-Beetle	S jadval	4→4 (bit)
7.	Romulus	S jadval	8→8 (bit)
8.	Sparkle	ARX almashtirish	-
9.	TinyJambu	NFSR	128 bit
10.	Xoodyak	Xoodoo χ akslantirishi	8x4→8x4 (bit)

Yuqoridagi tahlil natijalari taqdim etilgan algoritmlarning aksariyati S jadvalldan chiziqsiz akslantirish sifatida foydalanganidan dalolat berib, xususan, LWC uchun mos algoritmlarda 4x4 o‘lchamli S jadvallarni eng mosligini ko‘rish mumkin.

Nazariy savollari:

1. eSTREAM loyihasi, uning maqsadi, qatnashgan algoritmlar, loyiha natijalari haqida ayting?
2. CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) loyihasi, uning maqsadi, qatnashgan algoritmlar, loyiha natijalari haqida ayting?
3. NIST (National Institute of Standards and Technology) konkursi, uning maqsadi, o‘tkazish bosqichlari haqida ma’lumot bering?

4. ISO/IEC (International Organization of Standardization/ International Electrotechnical Commission) 29192 (Information technology — Security techniques — Lightweight cryptography) seriyali standart, belgilangan kriptografik algoritmlar haqida ma’lumot bering?

5. AEAD shifrlash, uning maqsadi?

6. CRYPTREC (Cryptography Research and Evaluation Committees) loyihasi, uning maqsadi, tanlab olingan algoritmlar haqida ma’lumot bering?

7. NIST konkursi finalchi algoritmlarining aksariyati qaysi konstruksiya asosida qurilgan?

8. NIST konkursi finalchi algoritmlarining chiziqsiz akslantirishlari xususiyatlari haqida ayting?

9. ASCON algoritmi haqida ayting?

10. Yengil vaznli shifrlash algoritmlarida chiziqli akslantirish sifatida qanday funksiyalardan foydalanilgan?

Adabiyotlar va Internet resurslar:

1. Xudoykulov, Z., & Rahmatullayev, I. (2024). Yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlash tahlili. Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий, 7(2), 51–58. извлечено от https://ijdt.uz/index.php/ijdt/article/view/181

2. https://en.wikipedia.org/wiki/ESTREAM - eSTREAM

3. https://en.wikipedia.org/wiki/CAESAR_Competition - CAESAR Competition

4. https://csrc.nist.gov/projects/lightweight-cryptography - Lightweight Cryptography

5. https://cdn.standards.iteh.ai/samples/78477/eeb8160165e94018828239d3fc6478a3/ISO-IEC-29192-2-2019.pdf

6. https://www.cryptrec.go.jp/en/about.html - About CRYPTREC

4-ma’ruza. YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLARNI QURISH, SAMARALI APPARAT VA DASTURIY AMALGA OSHIRISH USULLARI (2 соат)

Reja:

4.1. Yengil vaznli blokli simmetrik shifrlash algoritmlarini loyihalash usullari

4.2. Mavjud yengil vaznli kriptografik algoritmlarning apparat va dasturiy amalga oshirilish natijalariga ko‘ra tahlili.

Tayanch iboralar: *ARX (Addition/Rotation/XOR), WTS (wide-trail strategy), (Long Trail Strategy), Gibrid, Bitslice, involutiv usul, ultra yengil usul, GE (Gate equalent).*

4.1. Yengil vaznli blokli simmetrik shifrlash algoritmlarini loyihalash usullari

Simmetrik blokli shifrlarni IoT qurilmalariga moslashtirish uchun ko‘plab usullar, masalan, ARX (Addition/Rotation/XOR), WTS (wide-trail strategy), (Long Trail Strategy), Gibrid, Bitslice, involutiv usul, ultra yengil kriptografik algoritmlar. ARX usulida qurilgan algoritmlar asosan xotiradan foydalanishni minimallashtirishni maqsad qiladi. Bunga asosan uchta amaldan: modul bo‘yicha qo‘shish, aylantirish (rotate) va XOR, foydalanish bilan erishiladi. WTS usulida yuqori xavfsizlik darajasiga ega yengil kriptografik algoritmni qurish maqsad qilinadi. Buning uchun esa S jadvallardan va chiziqli funksiyalardan foydalanishga katta e’tibor beriladi. LTS usulida yuqori xavfsizlik darajasini saqlab qolgan holda kam xotira sarfiga erishishga harakat qilinib, odatda bu ARX va WTS usullarini mujassamlashtirish orqali amalga oshiriladi. Bitslice usulida kriptotizim funksiyalari bir bitli mantiqiy amallar shaklida ifodalanib, keyinchalik ular bitli amallar yordamida funksiyaning bir nechta nusxalarini parallel ravishda bajarish orqali amalga oshiriladi. Shundan qilib, *n* bitli protsessorda mantiqiy ko‘rsatma kriptotizimni ishlash vaqtini tezlashtiradigan *n* mantiqiy amallarning parallel bajarilishiga mos keladi. Involyutiv usul involyusion amallar majmuasidan foydalanilgani bilan xarakterlanib, bunda deshifrlashda ishlatiladigan amallarni shifrlashdagi bilan bir xil bo‘ladi. Buning natijasida amallarni saqlash uchun xotiradan foydalanish kamayadi. Gibrid usul yuqori xavfsizlikni ta’minlash, shifrlashda va deshifrlashda bir xil funksiyalardan foydalanish va ROM xotirasidan foydalanishni kamaytirish uchun o‘zida SPN va Feystel tarmoqlarini birlashtiradi. Quyida ushbu usullar haqida batafsil ma’lumotlar va ularga asoslangan algoritmlarning qiyosiy tahillari keltiriladi.

ARX usuli. Ushbu usulga asoslangan algoritmlarga xesh funksiyalarga Skein, BLAKE, oqimli shifrlash algoritmlariga Salsa20, ChaCha20, blokli simmetrik shifrlash algoritmlariga Hight, Simon, Speck, Lea va Chaskey- larni misol keltirish mumkin. Ushbu usulga xos bo‘lgan ikkita jixat mavjud: blok, kalit o‘lchamlarini protsessor registori o‘lchamiga moslashtirish mumkinligi (8, 16, ...). Masalan, High algoritmida kirish bloki 8 bitli 8 ta qismga ajratiladi va bu 8 bitli protsessorga moslashuvchan qiladi. Lea algoritmi esa kirish blokini 32 bitli 4 ta qismga ajratadi va bu algoritmni 32 hamda 64 bitli protsessorlar uchun moslashuvchan qiladi. Speck va Simon algoritmlari esa kirish blokini ikki qismga ajratadi. Speck va Simon

algoritmlari oilasi AQShning National Security Agency (NSA) tomonidan yaratilgan bo‘lib, ARX usuliga asoslangan asosiy algoritmlardan hisoblanadi.

Ushbu algoritmlarning turli blok va kalit uzunliklariga ega variantlari mavjud bo‘lib, ulardagi farqlar vaqtga, sarflangan xotira qiymati va xavfsizlik darajasiga ta’sir qiladi. Blok uzunligi qanchalik katta bo‘lsa, xotira shuncha ko‘p sarflanadi va xavfsizlik darajasi shuncha yuqori bo‘ladi. Xuddi shu fikrni kalit uzunligi uchun ham ishlatish mumkin. ARX kriptotizimi raundlar sonini oshirish orqali xavfsizlikni kafolatlasada, algoritmning umumiy ishlashiga salbiy ta’sir o‘tkazadi.

WTS usuli. Ushbu usul yuqorida aytilgan kabi yuqori xavfsizlik darajasiga ega bo‘lgan yengil kriptografik algoritmlarni yaratishni maqsad qilib, buning uchun S jadvallar va chiziqli akslantirishlarga katta e’tibor qaratadi. Ushbu usulga asosan yaratilgan algoritmlarga mCrypton, Present, Led, Zorro, Skinny, Born va Gift, misol keltirish mumkin. Ushbu algoritmlar orasida farq xabar va kalit o‘lchamlari, raundlar soni va bloklar ko‘rinishida (bit, matritsa, bitlar to‘plami, baytlar to‘plami va hak.) bo‘lib, ular amalga oshirishda turli natijalarni taqdim qiladi. Ushbu usulga asoslangan algoritmlar orasida eng mashhuri Present bo‘lib, u 2012-yilda standartlashtirilgan (ISO/IEC 29192-2) yengil blokli simmetrik shifrlash algoritmi hisoblanadi. Ushbu algoritmda blok uzunligi 64 bit, kalit uzunliklari 80 va 128 bit bo‘lib, 31 raundli SPN tarmog‘iga asoslangan. Ushbu algoritm yengil komponentlardan tashkil topgani bois, uni apparat amalga oshirish qulay.

LTS usuli. Ushbu usul WTS va ARX usullari kombinatsiyasiga asoslangani bois, yuqori darajali xavfsizlikni saqlash bilan xotiradan foydalanishni optimallashtirni maqsad qiladi. Xususan, LTS usulida modul bo‘yicha qo‘shish, aylantirish va XOR amallari orqali ifodalangan S jadvaldan, WTS usulidagi kabi chiziqli akslantirishlaridan foydalaniladi. Ushbu usulda yaratilgan mashhur algoritmlardan biri bu Sparx algoritmi bo‘lib, uning qator variantlari mavjud: Sparx-64/128, Sparx-128/128 va Sparx-128/256. Ushbu algoritmda 3 ta amaldan: 16 bit modulda qo‘shish, 16 bitli XOR amali va o‘nga va chapga aylantirish, foydalanilgan.

Bitslice usuli. Ushbu usulda kriptototizim funksiyalari bir bitli mantiqiy amallar nuqtai nazaridan ifodalanib, keyinchalik ular bitli amallar yordamida funksiyaning bir necha nusxalarini parallel ravishda bajarish orqali amalga oshiriladi. Xususan, *n* – bitli protsessorda mantiqiy ko‘rsatma kriptotizimni ishlash vaqtini tezlashtiradigan *n* mantiqiy amallarni parallel bajarilishiga mos keladi. Ushbu usulga asoslangan algoritmlarga Rectangle, Fantomas va Mysterion-larni misol keltirish mumkin. Masalan, Rectangle algoritmida blok o‘lchami 64 bit va kalit uzunligi 80 bit bo‘lib, 25 raunddan iborat va u SPN arxitekturasiga asoslangan. Raund funksiyasi raund kaliti bilan XOR amalida qo‘shish, 4×4 S jadval asosida o‘rniga qo‘yish, bit bo‘yicha surish amallaridan iborat bo‘lib, so‘ngi raunddan so‘ng raund kaliti bilan yana bir XOR amalida qo‘shish amalga oshiriladi. Ushbu usulning asosiy maqsadi RAM sarfini kamaytirish orqali ishlashni yaxshilashdan iborat bo‘lib, xavfsizlik darajasi tizimni amalga oshirishda foydalanilgan komponentga bog‘liq bo‘ladi.

Involyutiv usul. Ushbu usul, aytaylik, $f_i\big(f_i(x)\big) = x$ ko‘rinishidagi involyutiv funksiyalar to‘plamidan foydalanish bilan tavsiflanadi. U esa shifrlash va deshifrlash jarayonida foydalanilgan funksiya bir xil ekanligini anglatadi. Bu esa amallarni

saqlash uchun xotiradan foydalanishni kamayishiga olib keladi. Ushbu usulga asoslangan algoritmlarga Prince, Klein, Midori va Mantis-larni misol keltirish mumkin. Ushbu algoritmlar asosan kiritilgan involyutiv funksiyalar sonidan farq qilib, xususan, Prince, Midori algoritmlarida barcha amallar involyutiv bo‘lsa, Klein algoritmida faqat o‘rniga qo‘yish akslantirishi involyutiv hisoblanadi. Kriptografiyada involyutiv funksiyalardan foydalanish xotira sarfini kamaytirsada, xavfsizlik darajasini ham tushiradi. Masalan, Prince algoritmi 11 raund bo‘lib, SPN tarmoqqa asoslangan. Raund akslantirishi raun kaliti bilan XOR amalida qo‘shish va 4×4 S jadvallar asosida o‘rniga qo‘yishni amalga oshiriladi. Ushbu usulda ham Bitslice usuli kabi tezkorlik va ROMdan foydalanish amalga oshirilgan komponentni tanlashga bog‘liq.

Gibrid usul. Ushbu usul o‘zida SPN va Feystel tarmog‘larini mujassamlashtirgan bo‘lib, shifrlash va deshifrlashda yagona funksiyadan foydalanish orqali ROMdan foydalanishni kamaytirish bilan birga yuqori xavfsizlik darajasini saqlab qolishga harakat qiladi. Ushbu usulga asoslangan algoritmlarga Sea, Gost revisited, Celfia, Twine, Lblock, Piccolo, ITUbee, RoadRunner, LiCi, SIT, ANU-II va Nux, larni misol keltirish mumkin. Ushbu kriptotizimlar o‘rtasidagi asosiy farq shundaki, ular SPN tuzilishiga kiritilgan chiziqli sathdan foydalanadi. Twine va Gost revisited algoritmlaridan farqli ravishda Sea, Piccolo, RoadRunner, Lici va Nux algoritmlarida murakkab (amalga oshirish qimmat) chiziqli sathlardan foydalanilgan. O‘z navbatida ushbu sath aralashtirishning yuqori darajasini ta’minlashga xizmat qiladi. Gibrid usul SPN va Feystel tarmoqlariga asoslangan bo‘lib, yuqori xavfsizlik darajasini ta’minlash bilan birga katta xotira hajmini ham talab etadi. Mazkur holda gibrid usullarga asoslangan shifrlarning tezligi ularning raundlar soniga bog‘liq bo‘ladi.

O‘ta engil usul (Ultra-lightweight method, ULM). Yuqorida keltirilgan nazariy tadqiqotlar xavfsizlik darajasi, tezlik, ROM va operativ xotira istemoli o‘rtasida aniq bog‘lanishni ko‘rsatdi. Yuqorida keltirilgan usullar ushbu ko‘rsatkichlarning bir yoki ikkitasiga e’tibor qaratgan. Ushbu cheklovlarni bartaraf etish uchun mualliflar tomonidan ULM usuli taklif etilgan. Ushbu usulning asosiy maqsadi yuqori xavfsizlik darajasini, kriptoalgoritmning yaxshi ishlashi va kam xotira sarfini ta’minlash bo‘lib, buni amalga oshirish uchun usul o‘zida Bitslice, WTS va Involyutiv usullarni mujassamlashtiradi. Ushbu usul quyidagilar bilan xarakterlanadi:

1. Yuqori xavfsizlikni ta’minlash uchun aralashtirishni (diffusion) amalga oshirishda chiziqli funksiyalardan, chalkashtirishni (confusion) amalga oshirish uchun S jadvaldan foydalanish.
2. Algoritm tezkorligini ta’minlash foydalanilgan funksiyalarni bir bitli mantiqiy amallar nuqtai nazaridan ifodalash hamda ularni ushbu funksiyalarni bir nechta nusxalarini protsessorga parallel ravishda bajarish orqali erishiladi.
3. Involyutiv amallardan foydalanish orqali amallarni saqlash uchun xotiradan foydalanishni kamaytirish.

Mualliflar tomonidan taqdim etilgan ULM usulida asoslangan tizim ULC (Ultra-Lightweight Cryptosystem) deb nomlanadi. Ushbu algoritm Arduino Uno

platformasida amalga oshirilgan.

Yuqorida keltirilgan barcha usullar apparat yoki dasturiy ko‘rinishda amalga oshirilishidan qat’iy nazar hisoblash va quvvat imkoniyati cheklangan muhitlarda foydalanish uchun qaratilgan. 4.1-jadvalda ushbu usullarning qiyosiy tahlili keltirilgan.

4.1-jadval

Ko‘rib o‘tilgan usullarning xususiyatlari

Usul/ Xususiyat	**ARX Speck**	**WTS Present**	**LTS Sparx**	**Bitslice Rectangle**	**Involyutiv Prince**	**Gibrid LBlock**	**ULM ULC**
Struktura	Feystel	SPN	SPN+ARX	SPN	SPN	Feystel+ SPN	WTS+Bitslice+Involyutiv
Raund kalitlarini hosil qilish	Murakkab	Sodda	Murakkab	O‘rtacha	Sodda	Murakkab	Sodda
Apparat amalga oshirish	Yo‘q	Ha	Yo‘q	Ha	Ha	Ha	Ha
Dasturiy amalga oshirish	Ha	Yo‘q	Ha	Ha	Yo‘q	Ha	Yo‘q
O‘rniga qo‘yish	Bor	Bor	Bor	Bor	Bor	Bor	Bor
O‘rin almashtirish	Yo‘q	Bor	Bor	Bor	Bor	Bor	Bor
SWAP	Bor	Yo‘q	Bor	Yo‘q	Bor	Bor	Yo‘q
Ko‘paytirish	Yo‘q	Yo‘q	Yo‘q	Yo‘q	Bor	Yo‘q	Yo‘q
Siljitish	Yo‘q	Yo‘q	Ha	Yo‘q	Ha	Ha	Ha
1 va oxirgi raundda kalit bilan XOR amalida qo‘shish	Yo‘q	Yo‘q	Yo‘q	Yo‘q	Bor	Yo‘q	Bor
O‘zgarmasga qo‘shish	Yo‘q	Yo‘q	Yo‘q	Yo‘q	Bor	Yo‘q	Yo‘q
Raund kaliti bilan aralashtirish	Bor	Bor	Bor	Bor	Bor	Bor	Bor
Kalit o‘lchami (bit)	32 dan 128 gacha	80/128	128/256	80/128	128	80	80
Blok o‘lchami (bit)	32 dan 128 gacha	64	64/128	64	64	64	64
Raundlar soni	22 dan 34 gacha	31	24-40	25	12	32	15

Barcha yuqorida ko‘rib o‘tilgan usullarning xavfsizlik, amalga oshirish va xotiradan foydalanish ko‘rsatkichlari bo‘yicha tahlili 4.2-jadvalda keltirilgan.

4.2-jadval

Ko‘rib o‘tilgan usullarning qiyosiy tahlili

Usul	**Xavfsizlik darajasi**	**Amalga oshirish**	**RAM sarfi**	**ROM sarfi**
ARX	Past	O‘rtacha	Past	Neytral
WTS	Yuqori	Past	Past	Yuqori
LTS	Yuqori	Yuqori	Yuqori	Yuqori
Gibrid	Yuqori	Yuqori	Yuqori	O‘rtacha
Bitslice	Neytral	n bitli protsessor foydalanilsa, yuqori	Past	Neytral
Involyutiv	Past	Neytral	Yuqori	Past
ULM	Yuqori	Yuqori	Past	Past

Ushbu usullar asosida yaratilgan algoritmlarning amalga oshirishdan olingan natijalarning qiyosiy tahlili 4.3-jadvalda keltirilgan.

4.3-jadval

Algoritmlarning amalga oshirish natijalari

№	Omillar/ algoritmlar		Speck	Rectangle	Prince	LBlock	Sparx	ULC	Present
1.	64 bit uchun ishlash vaqti (ms)	Shifrlash	0.42	0.3	0.8	0.32	0.3	0.13	-
		Deshifrlash	0.42	0.31	0.8	0.32	0.31	0.13	-
2.	64 bit uchun ishlash sikli (clock cycle)	Shifrlash	6784	4736	12735.99	5120	4864	1230	-
		Deshifrlash	6784	4.928	12735.99	5120	4992	1231	-
3.	ROM sarfi (KB) (shifrlash/ deshifrlash)		3.0	3.2	2.5	3.4	4.2	2.2	4.4
4.	RAM sarfi (KB) (shifrlash/ deshifrlash)		$1.9*10^{-1}$	$1.9*10^{-1}$	$3.1*10^{-1}$	$3.1*10^{-1}$	$2.1*10^{-1}$	$2*10^{-1}$	$2*10^{-1}$
5.	Aralash-tirish (%)	Min	29	30	31	31	31.9	32	32
		O‘rtacha	49.98	50.1	50.1	51	49.9	50	50
		Max	69	69.1	69.1	70.1	68	67.9	68
6.	Chalkash-tirish (%)	Min	47.2	47.1	47.3	47.8	47.1	47.89	47.77
		O‘rtacha	49.97	49.9	50.1	49.89	49.89	50	50
		Max	52.29	53.1	53	52.2	52.2	52.2	52.4

4.2. Mavjud yengil vaznli kriptografik algoritmlarning apparat va dasturiy amalga oshirilish natijalariga ko‘ra tahlili

IoT tizimlari uchun mo'ljallangan kriptografik tizimlar “yengil vaznli” kriptografik algoritmlar deb ataladi va ularning xarakteristikalari amalga oshirish shakliga ko‘ra ISO/IEC 29192 standartida keltirilgan. Chip o‘lchami va quvvat sarfi apparatga asoslangan ilovalar uchun muhim omillar deb hisoblangan bo‘lsa, kod uzunligi va kichik RAM xotira hajmi dasturiy ta’minotga asoslangan ilovalar uchun muhim omillar deb hisoblanadi.

Tahlillash uchun tanlab olingan algoritmlar quyidagilar:

Simmetrik blokli shifrlar. Hozirgacha ko‘plab engil blokli shifrlash algoritmlari taklif qilingan. Xususan, CLEFIA [2] va PRESENT [3] algoritmlari

ham xavfsizlik, ham amalga oshirish bilan tavsiflanadi. Ikkala algoritm ham ISO/IEC 29192:2 ning bir qismidir va ko‘plab IoT qurilmalarida qo‘llaniladi. Umumiy yengil simmetrik blokli shifrlar va ularning tafsilotlari 4.4-jadvalda keltirilgan.

4.4-jadval

Yengil blokli shifrlarning xarakteristikalari

Algoritm	**Kalit o‘lchami (bit)**	**Blok o‘lchami (bit)**	**Roundlar soni**	**Yili**
SEA	*n* ga bog‘liq	*b ga bog‘liq, n=6b.*	≥ 3n/4	2006
HIGHT	128	64	32	2006
Hummingbird	256 bit kalit o‘lchami, 80 bit ichki blok o‘lchami	16	Blokli va oqimli shifrlashga asoslangan loyiha	2010
Hummingbird2	128, 64 bit initialization vector	16	Blokli va oqimli shifrlashga asoslangan loyiha	2012
PRESENT	80	64	31	2007
PRINTcipher	$\frac{5}{3} \times b$	$b \in \{48, 96\}$	b	2010
KATAN& KTANTAN	80	32, 48, 64	254	2009
mCrypton	64, 96, 128	64	12	2005
KLEIN	64, 80, 98	64	12, 16, 20	2011
TWINE	80, 128	64	36	2013
SIMON& SPECK	64, {72, 96}, {96, 128}, {96, 144}, {128, 192, 256}	32, 48, 64, 96, 128	32, 36, {42, 46}, {52, 54}, {68, 69, 72}	2013
PRINCE	128	64	12	2012
PRIDE	128	64	19	2012
LBLOCK	80	64	32	2011
MIBS	46, 80	64	32	2009
Puffin	128	64	32	2011
ESF	80	64	32	2014
Piccolo	80, 128	64	25, 31	2011
Khudra	80	64	18	2014

Oqimli shifrlar. ECRYPT II eSTREAM loyihasining bir qismi sifatida ko‘plab oqim shifrlari tanlangan. Umumiy yengil shifrlash algoritmlariga misollar 4.5-jadvalda keltirilgan.

4.5-jadval

Yengil oqimli shifrlarning xarakteristikalari

Algoritm	**Kalit o‘lchami (bit)**	**Blok o‘lchami (bit)**	**Initialization vector**	**Yil**
RC4	8-2048	1	-	1987
A5/1	54, 64	-	0	1989
E0	128	-	0	1998
Rabbit	128	128	-	2003
Grain	80, 128	1, 16	64, 96	2004
Triviu	80	1, 8, 16	80	2004
Salsa	128, 256	32, 512	64, 128	2004
HC	128, 256	-	128, 256	2004
Enocoro	80, 128	1	64	2008
Rabbit-MA	128	128	-	2008
BEAN	80	2	64	2009
WG-7	80	1	81	2010
TinyStream	128	-	-	2010
Grain-128a	128	1	96	2011
A2U2	56	1	-	2011
Quavium	80	1	80	2012
Cavium	80	1	80	2012

ASC-1	128	128	56	2012
WG-8	80	1, 11	80	2013
CAR30	128	128	120	2013
ALE	128	128	128	2013
ACORN	128	-	128	2014
Sablier	80	-	80	2014

Xesh funksiyalar. Mavjud xesh-funksiyalar, xususan, SHA-3 oilasining algoritmlari IoT talablariga javob bermasligi sababli, yengil xesh-funksiyalarni yaratish ushbu sohadagi dolzarb masalalardan biridir. Umumiy yengil xesh funksiyalar 4.6-jadvalda keltirilgan algoritmlarni o‘z ichiga oladi.

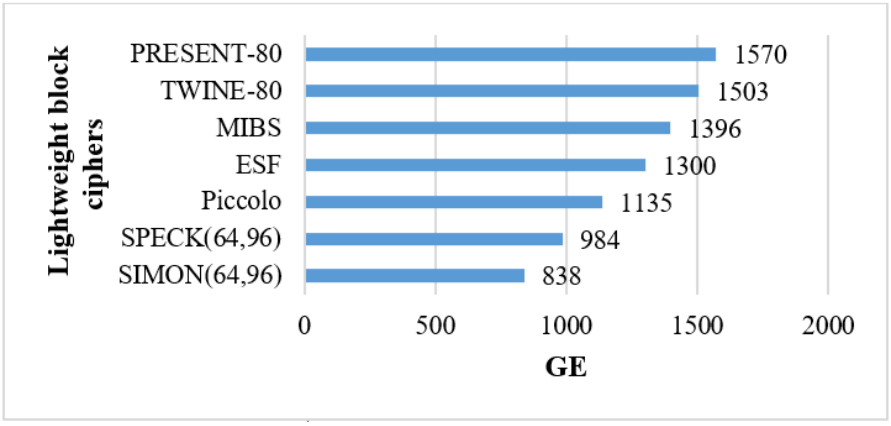
4.6-jadval

Yengil xesh funksiyalarning xarakteristikalari

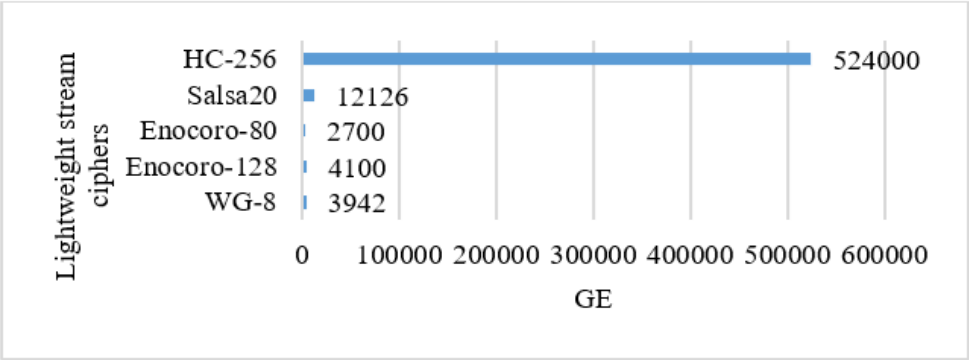
Xesh funksiyalar	**Xesh qiymat uzuligi (bit)**	**Konstruksiya**	**Yil**
PRESENT (xeshlash rejimida)	64	Davies-Meyer mode	-
PHOTON	64≤ n ≤256	Sponge-like construction	2011
SPONGENT	88, 128, 160, 224, 256	Sponge-like construction	2013
Keccak	64, 128, 256	Sponge-like construction	2010
Quark	136, 176, 256	Sponge-like construction	2010
Neeva	224	Sponge-like construction	2016
GLUON	128, 160, 224	Sponge-like construction	2012
ARMADILLO	48	Merkle–Damgård	2010
Lesamnta-LW	256	Merkle–Damgård	2010

Yengil vaznli shifrlarni xarajat nuqtai nazaridan baholash

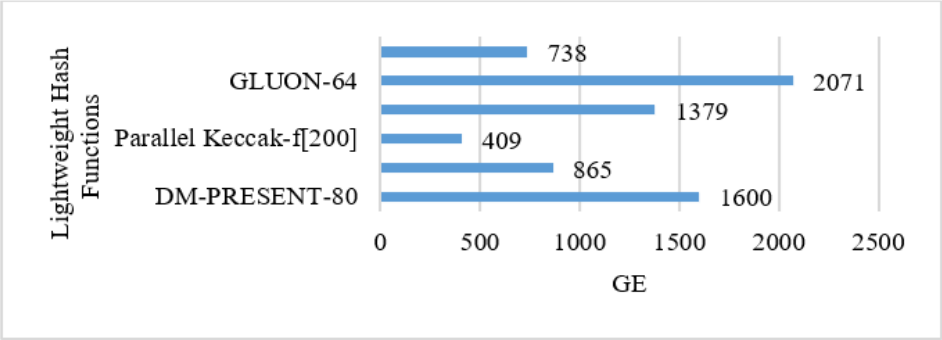
Apparat amalga oshirish. Yengil kriptografik algoritmlarni apparat yordamida amalga oshirish narxi mikrosxemaning o‘lchami yoki zarur bo'lgan mantiqiy elementlarning soni bilan belgilanadi: bu miqdor qanchalik kichik bo‘lsa, narx ham past bo‘ladi. Kritik maydon odatda μm^2 birliklarida hisoblanadi. Biroq, bu o‘lchov ishlab chiqarish texnologiyasiga bog‘liq. Shuning uchun ishlab chiqarish texnologiyasidan qat’i nazar, eshik ekvivalenti (GE) o‘lchov turidan foydalanish tavsiya etiladi. 4.1-rasmda yengil blokni, oqimni shifrlash algoritmlarini va xesh-funksiya algoritmlarini apparatni amalga oshirish uchun zarur bo‘lgan GE miqdori ko‘rsatilgan.



a) Yengil blokli shifrlar



b) Yengil oqimli shifrlar



c) Yengil xesh funksiyalar

4.1-rasm. Apparat amalga oshirishda GE soni bo‘yicha taqqoslash

Dasturiy ko‘rinishda amalga oshirish. Dasturiy ko‘rinishda amalga oshirish narxi RAM (tasodifiy kirish xotirasi), ROM (faqat o‘qish uchun mo‘ljallangan xotira) va algoritmning kod hajmi bilan o‘lchanadi. 4.7-jadvalda RAM, ROM va Kod hajmini o‘lchash bilan dasturiy ta’minotni amalga oshirish bo‘yicha yengil shifrlar baholanadi.

4.7-jadval

O‘lchash uchun ishlatiladigan RAM, ROM va kod hajmi bo‘yicha dasturiy ta’minotni amalga oshirish xarajatlari nuqtai nazaridan yengil shifrlarni baholash

Turi	Algorithmlar	RAM	ROM	Kod o‘lchami
Oqimli shifrlar	Grain	20	778	-
	Trivium	36	424	-
	Salsa20	258	3842	1452
	WG-7	0	938	-
	WG-8	148	2238	-
Blokli shifrlar	KATAN-64	625	3260	338
	PRESENT-80	365	6866	936
	mCrypton-64	355	9768	1076
	TWINE	335	728	-
	SEA	249	1904	2132
	Hummingbird	159	2646	5100
	PRINCE	125	6184	1108
	HIGHT	117	2510	5100
	KLEIN-80	107	2672	2672

Tezlik nuqtai nazaridan yengil vaznli shifrlarni baholash

Yengil vaznli shifrlarning tezligini baholash o‘lchovlari apparatdagi blokdagi soat sikllari soni (clock cycles per block) va dasturiy ta’minotni amalga oshirishda bayt uchun tsikllardir (cycles per byte). Ushbu chora-tadbirlar yordamida yengil shifrlarni baholash natijalari quyidagicha bo‘ladi.

Apparatda amalga oshirish. Uskuna tezligi uchun engil shifrlarni baholashda blokdagi soat sikllari soni va talab qilinadigan vaqt eng muhim o‘lchovlardir. Vaqt

shkalasi bo‘yicha yengil vaznli shifrlarni to‘g‘ri baholash uchun ish chastotasi bir xil bo‘lishi kerakligi sababli, berilgan topshiriq uchun zarur bo‘lgan vaqt miqdori tsikllar sonini ish chastotasiga bo‘lish yo‘li bilan olinishi mumkin; bu o‘lchovni tsikllar soniga bog‘liq deb hisoblash mumkin. Baholashdan so‘ng, vaqt va tsiklning ushbu ko‘rsatkichlaridan biri etarli.

Dasturiy ko‘rinishida amalga oshirish. Yengil vaznli shifrlarning o‘lchovi - bu baytdagi soat sikllari soni. 4.8-jadvalda blok/bayt uchun soat sikllari bo‘yicha yengil shifrlarning apparat va dasturiy ta’minotni amalga oshirish tezligini baholash ko‘rsatilgan.

4.8-jadval

Tezlik nuqtai nazaridan yengil vaznli kriptografik algoritmlarni baholash

Turi	**Algorithmlar**	**Clock cycle per block (qurilma)**	**Clock cycle per byte (dasturiy ko‘rinishda)**
Blokli shifrlar	Hummingbird	1399	-
	KATAN-64	255	9007
	PRINT-48	768	-
	SEA	93	805
	TWINE	36	271
	HIGHT	34	307
	PRESENT-80	32	1199
	mCrypton	13	2057
Oqimli shifrlar	WG-8	1	69 (Shifrlash)
	Enocoro-128	1	138 (Shifrlash)
	Salsa20-128	2	29491 (Shifrlash)
	HC-128	-	17388 (Shifrlash)
Xesh funksiyalar	DM-PRESENT-80	4547	-
	PHOTON-80/20/16	708	-
	Parallel Keccak-f[200]	18	-
	U-Quark	544	-
	GLUON-64	66	-
	spongent-88/80/8	990	-

Apparat ko‘rinishda amalga oshirish xarajatlarini baholash SPECK, Enocoro-80 shifrlari va Kessak xesh funktsiyalari ustunligini ko‘rsatadi. Apparat amalga oshirish tezligi bo‘yicha baholash mCrypton, WG-8 va TWINE ning ustunligini ko‘rsatadi. WG-8 shifrlash dasturiy ta’minotni amalga oshirishda eng yaxshisi bo‘ldi.

Nazariy savollari:

1. ARX konstruksiyasiga qurilgan shifrlarni xususiyatlari haqida ayting?
2. WTS konstruksiyasiga qurilgan shifrlarni xususiyatlari haqida ayting?
3. LTS konstruksiyasiga qurilgan shifrlarni xususiyatlari haqida ayting?
4. Bitslice konstruksiyasiga qurilgan shifrlarni xususiyatlari haqida ayting?
5. Feystel tarmog‘i va uning asosiy afzalliklari haqida ma’lumot bering?
6. SP tarmog‘i va uning asosiy afzalliklari haqida ma’lumot bering?
7. Yengil vaznli algoritmlarni apparat amalga oshirish uchun qanday omillar muhim hisoblanadi?
8. Yengil vaznli algoritmlarni dasturiy amalga oshirish uchun qanday omillar muhim hisoblanadi?
9. GE qanday kattalik va qanday hisoblanadi?
10. Apparat va dasturiy ko‘rinishda amalga oshirishda tezlik qanday o‘lchanadi?

Adabiyotlar va Internet resurslar:

1. Худойкулов З.Т., Ортиқбоев А.М. Енгил блокли симметрик шифрлаш алгоритмларини лойиҳалаш усулларининг таҳлили. Ахбороткоммуникациялар: тармоқлар-технологиялар-ечимлар. АК: ТТЕ № 1 (65)/2023, С. 26-31

2. Khudoykulov, Z. (2024). A Comparison of Lightweight Cryptographic Algorithms. In: Aliev, R.A., et al. 12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022). WCIS 2022. Lecture Notes in Networks and Systems, vol 912. Springer, Cham. https://doi.org/10.1007/978-3-031-53488-1_36

3. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Rob-shaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P. and Verbauwhede, I. (eds.) Cryptographic Hard-ware and Embedded Systems - CHES 2007. pp. 450–466. Springer Berlin Heidelberg, Berlin, Heidelberg (2007).

4. Tareq Hammad, B., Jamil, N., Ezanee Rusli, M., Reza, M.Z.: A survey of Lightweight Cryptographic Hash Function. Int J Sci Eng Res. 8, (2017).

5. Hosseinzadeh, J., Hosseinzadeh, M.: A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers: Hardware and Software Implementation. Advances in Computer Science: An International Journal. 5, 31–41 (2016).

IV BO‘LIM.

AMALIY MASHG‘ULOT MATERIALLARI

IV. AMALIY MASHG‘ULOT MATERIALLARI

1-amaliy ish. ASCON ALGORITMI (4 soat)

Amaliy ishning maqsadi – Ascon algoritmi haqida nazariy bilim va uni dasturiy amalga oshirish bo‘yicha amaliy ko‘nikmalarni shakllantirishdan iborat.

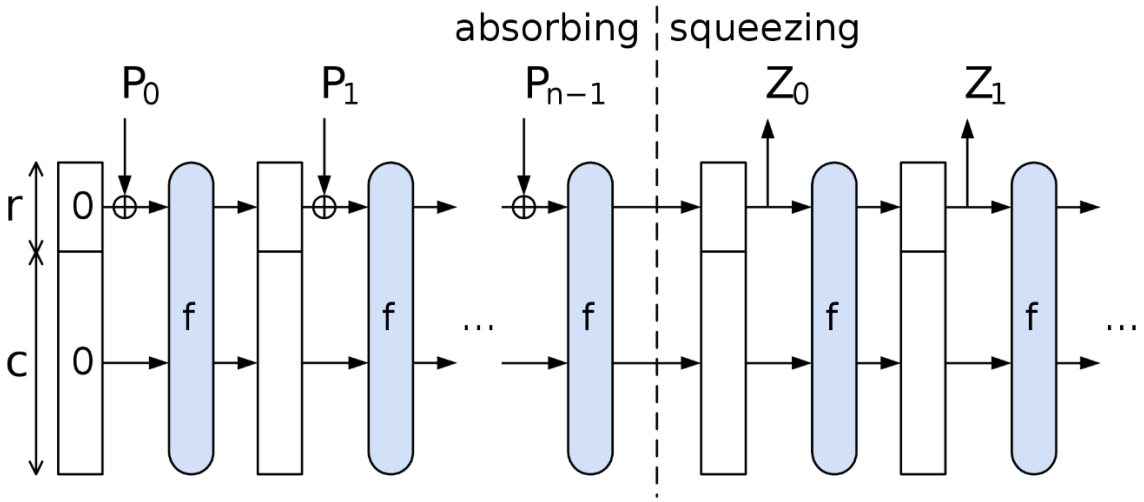
Nazariy qism

Ascon shifri AEAD turidagi shifrlash algoritmi bo‘lib, Sponge konstruksiyasiga asoslangan. Shu sababli, dastlab ushbu konstruksiya bilan tanishib chiqilad.

Sponge konstruksiyasi

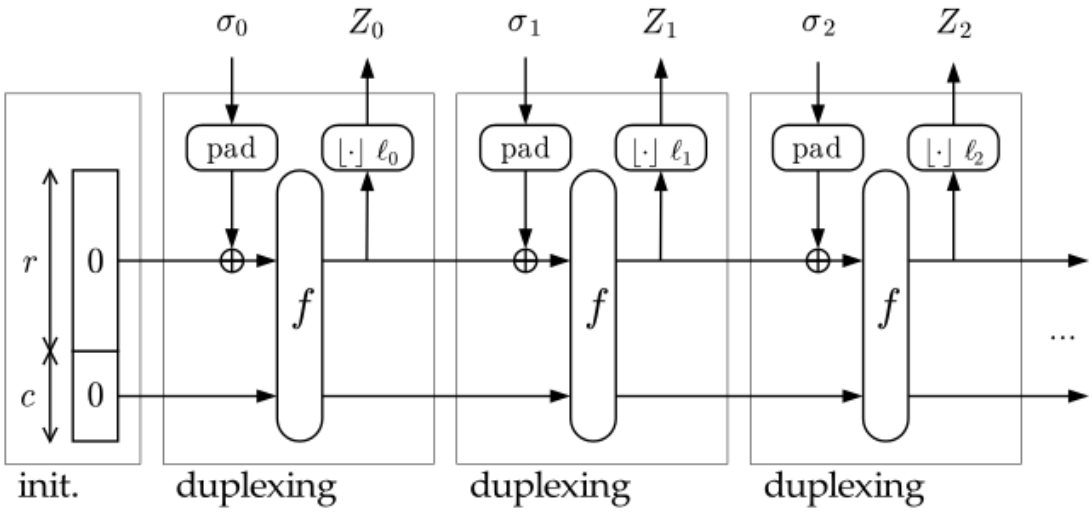
Kriptografiyada sponge (shimgich) funksiyasi yoki sponge konstruktsiyasi har qanday uzunlikdagi kirish bit oqimini oladigan va istalgan uzunlikdagi chiqish bit oqimini ishlab chiqaradigan chekli ichki holatga ega bo‘lgan algoritmlarning har qanday sinfidir. Sponge funktsiyalari ham nazariy, ham amaliy foydalanishga ega. Ular kriptografik xeshlar, xabar autentifikatsiya kodlari, oqimli shifrlar, psevdo-tasodifiy sonlar generatorlari va autentifikatsiyalangan shifrlash kabi ko‘plab kriptografik primitivlarni modellashtirish yoki amalga oshirish uchun ishlatilishi mumkin.

Sponge konstruksiyasining umumiy ko‘rinishi 1.1-rasmda keltirilgan. Ushbu konstruksiya 2 bosqichdan *absorbing* (singish) va *squeezing* (siqib chiqarish) iborat.



1.1-rasm. Sponge konstruksiyasi

Ushbu konsturksiyaning duplex rejimi ham mavjud bo‘lib, uning ko‘rinishi 1.2-rasmda keltirilgan.



1.2-rasm. Sponge duplex rejimi

Bundan tashqari, ushbu konstruksiyaning SpongeWrap va MonkeyDuplex kabi ko‘rinishlari ham mavjud. Ushbu konstruksiya asosida ko‘plab, mashhur xesh algoritmlari va shifrlash algoritmlari ishlab chiqilgan. Masalan, Keccak, Ascon shular jumlasidan.

Ascon algoritmi. Ascon - bu AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan yengil vaznli kriptografiyani kelajakda standartlashtirish uchun tanlangan yengilvaznli autentifikatsiyalanuvchi shifrlar oilasi.

Ascon 2014-yilda Grats Texnologiya Universiteti, Infineon Technologies, Lamarr Security Research va Radboud universiteti tadqiqotchilari jamoasi tomonidan ishlab chiqilgan. Shifrlar oilasi 2019-yil fevral oyida CAESAR tanlovining finalchisi sifatida tanlangan.

Loyiha monkeyDuplex va SpongeWrap kabi sponge ko‘rinishlaridagi konstruktsiyasiga asoslangan. Ushbu loyiha Ascondan bir necha usulda (shifr, xesh yoki MAC sifatida) qayta foydalanishni osonlashtiradi. 2023-yil fevral holatiga ko‘ra Ascon to‘plami ettita shifrni o‘z ichiga olgan, jumladan:

- Ascon-128 va Ascon-128a autentifikatsiyalovchi shifrlar;
- Ascon-Hash kriptografik xesh algoritmi;
- Ascon-Xof kengaytiriladigan-chiqish xesh funktsiyasi;
- Ascon-80pq shifrini post kvant hisoblash qurilmalari uchun “takomillashgan” 160 bitli kalitga ega shakli.

Asosiy komponentlar boshqa loyihalardan olingan:

- chiziqsiz qatlam Keccakning χ funktsiyasidan o‘zgartirilgan S-boxdan foydalanadi;
- chiziqli qatlami funksiyalari SHA-2 ning Σ funksiyasiga o‘xshash.

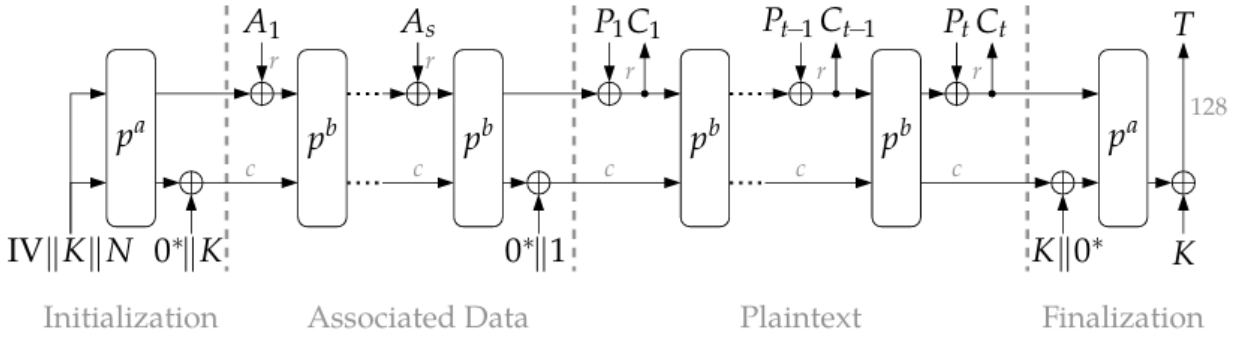
Ascon algoritmining autentifikatsiyalanuvchi shifrlash rejimida foydalanilgan parametrlar quyidagicha:

Name	Algorithms	Bit size of				Rounds	
		key	nonce	tag	data block	p^a	p^b
Ascon-128	$\mathcal{E}, \mathcal{D}_{128,64,12,6}$	128	128	128	64	12	6
Ascon-128a	$\mathcal{E}, \mathcal{D}_{128,128,12,8}$	128	128	128	128	12	8

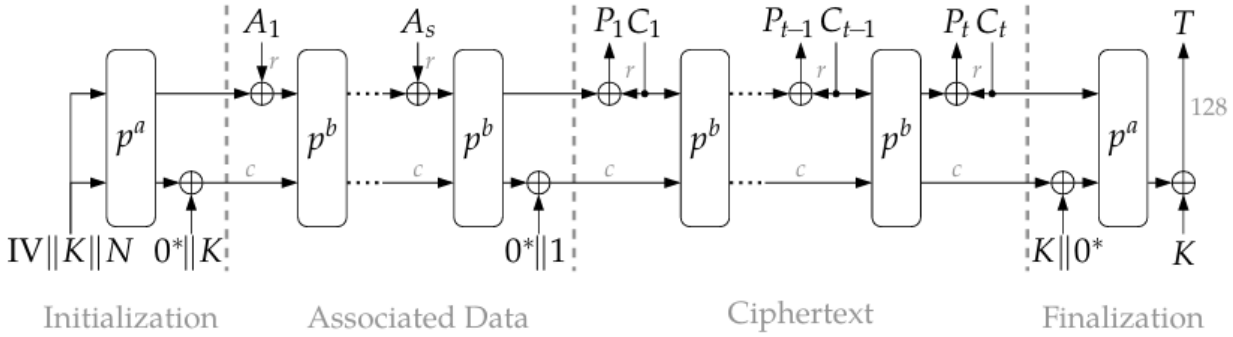
Xeshlash rejimi uchun esa quyidagicha:

Name	Algorithm	Bit size of		Rounds
		hash	data block	p^a
Ascon-Hash	$\mathcal{X}_{256,64,12}$ with $\ell = 256$	256	64	12

Ascon algoritmining autentifikatsiyalanuvchi shifrlash rejimidagi shifrlash/ deshifrlash jarayoni quyida keltirilgan:

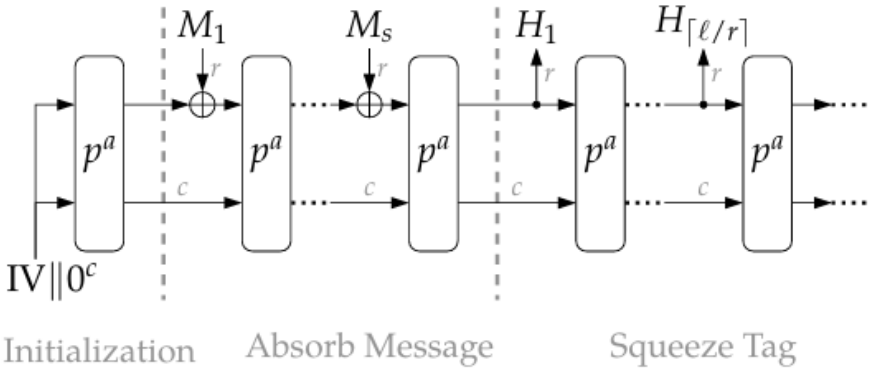


(a) Encryption $\mathcal{E}_{k,r,a,b}$



(b) Decryption $\mathcal{D}_{k,r,a,b}$

Xeshlash jarayoni esa quyidagicha:



Amaliy qism

Ascon algoritmini dasturiy amalga oshirish uchun va uni ishlash tartibi tushunish uchun mavjud bo‘lgan Python dasturlash tilidagi ishlanmalardan foydalanildi. Xususan, buning uchun https://github.com/meichlseder/pyascon manzildagi pyascon nomli ishlanmadan foydalanilgan.

Buning uchun ko‘rsatilgan manzildan loyihani ko‘chirib olish, uni ishga

tushurish tartibi bilan tanishib chiqing.

Ascon algoritmining barcha variantlaridan foydalanib, u haqida amaliy ko‘nikmalarni shakllantiring.

Amaliy bajarish uchun vazifalar

Yuqorida keltirilgan koddan foydalangan holda quyidagilarga javob bering:

1. AEAD rejimi uchun yozilgan shifrlash va deshifrlash funksiyasini turli ma’lumot uzunliklari uchun bajarilish vaqtini (millisekundda) hisoblang.
2. Xuddi shuningdek, xeshlash algoritmlari uchun ham vaqtni hisoblang.
3. Algoritmdan foydalanib, turli uzunlikdagi, 32, 64, 96 bitli xesh qiymatlarni hosil qiling.

Adabiyot va Internet saytlar:

1. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf - Ascon v1.2
2. https://en.wikipedia.org/wiki/Sponge_function - Sponge function
3. https://keccak.team/sponge_duplex.html - The sponge and duplex constructions
4. https://github.com/meichlseder/pyascon - Python implementation of Ascon

2-amaliy ish. PRESENT ALGORITMNI (2 soat)

Amaliy ishning maqsadi – tinglovchilarda shifrlash algoritmlarini dasturiy amalga oshirish ko‘nikmasini shakllantirishdan iborat.

Nazariy qism

PRESENT - SP tarmog‘iga asoslangan o‘ta engilvaznli blokli shifrlash algoritmi. PRESENT juda ixcham va apparatda samarali bo‘lishi uchun yaratilgan. U 64 bitli bloklarda va 80 yoki 128 bitli kalitlar bilan ishlaydi. U kam quvvat istemoli va yuqori chip samaradorligi talab qilinadigan holatlarda foydalanish uchun mo‘ljallangan, shuning uchun uni cheklangan muhitlar uchun alohida ahamiyatga ega. PRESENT-ning asosiy loyihalash maqsadi, boshqa engil shifrlarda bo‘lgani kabi, soddalikdir. PRESENT 31 raundda amalga oshiriladi, ularning har biri uch bosqichdan iborat (2.1-rasm):

• kalit bilan aralashtirish: XOR amali bo‘yicha qo‘shish va shundan so‘ng kalitni 61-bitli aylantirish orqali kalitlarni yangilash;

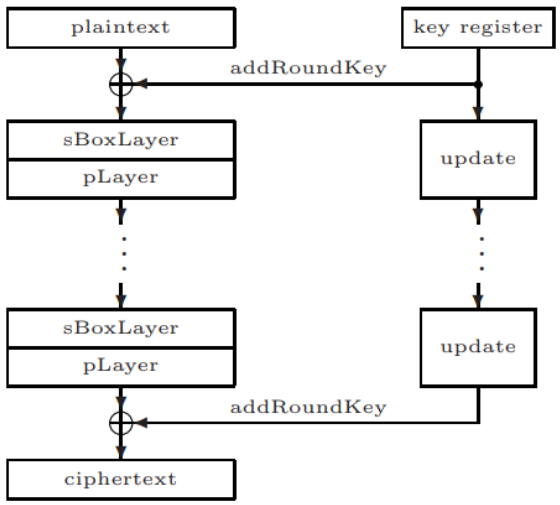
• o‘rniga qo‘yish qatlami, 16 ta 4-bitli (kirish) 4-bitli (chiqish) S jadvallari orqali;

• o‘rin almashtirish qatlami.

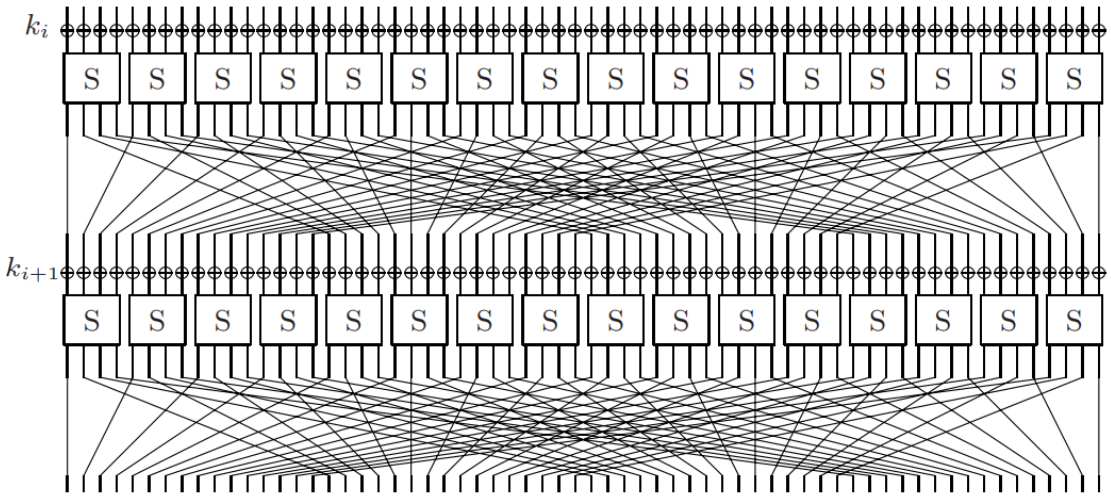
31-raund oxirida qo‘shimcha raund oxirgi raundning qism kalitini XORlash orqali amalga oshiriladi.

Algoritm qabul qilingan *ISO/IEC 29192-2:2012 Lightweight Cryptography* nomlari engil vaznli kriptografiya uchun mos blokli shifr sifatida qabul qilingan.

generateRoundKeys()
for $i = 1$ to 31 **do**
  addRoundKey(STATE,K_i)
  sBoxLayer(STATE)
  pLayer(STATE)
end for
addRoundKey(STATE,K_{32})



2.1-rasm. PRESENT algoritmining qisqa ko‘rinishi



2.2-rasm. PRESENT uchun SP tarmoq

31 raundning har biri raund kaliti K_i $(1 \leq i \leq 32)$ bilan XOR amalida qo‘shish (K_{32} qo‘shimcha raundda ishlatiladi (post-whitening)), bit darajasida chiziqli almashtirish va chiziqsiz akslantirish (S jadval) amallaridan iborat. Chiziqsiz akslantirish bosqichida 4 bitli S jadval har bir raund uchun parallel ravishda 16 marta ishlatiladi.

addRoundKey. Berilgan $K_i = \kappa_{63}^i \dots \kappa_0^i$ $(1 \leq i \leq 32)$ raund kaliti va joriy holat (STATE) $b_{63} \dots b_0$ da $0 \leq j \leq 63$ lar uchun addRoundKey quyidagicha bajariladi:

$$b_j \to b_j \oplus \kappa_j^i$$

sBoxlayer. Present algoritmida foydalanilgan S jadval 4 bit kirish va 4 bit chiqishni amalga oshiradi: $F_2^4 \to F_2^4$. S jadvalning 16 sanoq tizimidagi ifodasi quyida keltirilgan:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

sBoxlayer sathi uchun joriy STATE $b_{63} \dots b_0$ - 16 ta $w_{15} \dots w_0$ 4 bitli so‘zlardan iborat, bu yerda, $0 \leq i \leq 15$ uchun $w_i = b_{4*i+3} \parallel b_{4*i+2} \parallel b_{4*i+1} \parallel b_{4*i}$ va chiqish $S[w_i]$ esa yangilangan holat qiymatlarini taqdim etadi.

pLayer. PRESENT algoritmida foydalanilgan bitlarni almashtirish quyidagi jadvalga berilgan. STATEning i – biti $P(i)$ pozitsiyadagi bitga ko‘chiriladi.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Raund kalitlarni hosil qilish. PRESENT algoritmida kalit uzunligi 80 yoki 128 bitli bo‘ladi. Hozir esa 80 bit kalit holati qarab chiqiladi. Dastlabki kalit K kalit

registrida saqlanadi va $k_{79}k_{78}\dots k_0$ shaklida taqdim etiladi. i-raunddagi 64-bitli raund kaliti $K_i = \kappa_{63}\kappa_{62}\dots\kappa_0$ registrda saqlangan kalit K ning joriy qiymatining chap tomondagi 64 bitidan iborat bo‘ladi. Shuning uchun i raundda quyidagiga ega bo‘linadi:

$$K_i = \kappa_{63}\kappa_{62}\dots\kappa_0 = k_{79}k_{78}\dots k_{16}.$$

Raund kaliti K_i ajratilganidan so‘ng, kalit registori $K = k_{79}k_{78}\dots k_0$ quyidagicha yangilanadi:

1. $[k_{79}k_{78}\dots k_1k_0] = [k_{18}k_{17}\dots k_{20}k_{19}]$
2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus \texttt{round\_counter}$

Shunday qilib, kalit registori 61 bit chapga aylantiriladi va chapdagi eng chetki 4 bit S jadvaldan o‘tkaziladi va round_counter qiymati i o‘ng tomondan boshlab (Least significant bit, LSB) XOR amalida K kalitning $k_{19}k_{18}k_{17}k_{16}k_{15}$ bitlariga qo‘shiladi.

Amaliy qism

PRESENT shifrini Python dasturlash tilida amalga oshirildi.

1. Dastlab shifrning har bir akslantirishlarini funksiya sifatida hosil qilamiz.

1.1. Chiziqsiz akslantirish, S jadvalni statik ravishda (LUT jadval sifatida) e’lon qilamiz.

```
#        0   1   2   3   4   5   6   7   8   9   a   b   c   d   e   f
Sbox= [0xc,0x5,0x6,0xb,0x9,0x0,0xa,0xd,0x3,0xe,0xf,0x8,0x4,0x7,0x1,0x2]
```

1.2. SP tarmog‘iga asoslangan shifrlar uchun deshifrlash jarayonida akslantirishlarning teskarisi talab etiladi. Shu bois S jadval uchun teskari S jadval quyidagi kod yordamida hosil qilinmoqda.

```
Sbox_inv = [Sbox.index(x) for x in range(16)]
```

1.3. P jadval ham shifrlash jarayoni uchun statik ravishda taqdim etiladi.

```
PBox = [0,16,32,48,1,17,33,49,2,18,34,50,3,19,35,51,
        4,20,36,52,5,21,37,53,6,22,38,54,7,23,39,55,
        8,24,40,56,9,25,41,57,10,26,42,58,11,27,43,59,
        12,28,44,60,13,29,45,61,14,30,46,62,15,31,47,63]
```

1.4. Unga mos teskari P jadval ham kod yordamida quyidagicha hosil qilinadi:

```
PBox_inv = [PBox.index(x) for x in range(64)]
```

2. 80 va 128 bitli holatlar uchun raund kalitlarini hosil qilish.

2.1. 80 bitli kalitdan 32 ta raund kalitlarin hosil qilish.

```
def generateRoundkeys80(key,rounds):
        roundkeys = []
        for i in range(1,rounds+1): # (K1 ... K32)
                # rawkey: used in comments to show what happens at bitlevel
                # rawKey[0:64]
                roundkeys.append(key >>16)
                #1. Shift
                #rawKey[19:len(rawKey)]+rawKey[0:19]
                key = ((key & (2**19-1)) << 61) + (key >> 19)
                #2. SBox
                #rawKey[76:80] = S(rawKey[76:80])
                key = (Sbox[key >> 76] << 76)+(key & (2**76-1))
                #3. Salt
                #rawKey[15:20] ^ i
                key ^= i << 15
        return roundkeys
```

2.2. 128 bitli kalit uchun raund kalitlarini hosil qilish.

```
def generateRoundkeys128(key,rounds):
        roundkeys = []
        for i in range(1,rounds+1): # (K1 ... K32)
                # rawkey: used in comments to show what happens at bitlevel
                roundkeys.append(key >>64)
                #1. Shift
                key = ((key & (2**67-1)) << 61) + (key >> 67)
                #2. SBox
                key = (Sbox[key >> 124] << 124)+(Sbox[(key >> 120) & 0xF] << 120)+(key & (2**120-1))
                #3. Salt
                #rawKey[62:67] ^ i
                key ^= i << 62
        return roundkeys
```

3. Raund akslantirishlari quyidagi 3 ta boshqichdan iborat.

3.1. Birinchi akslantirish raund kalitlarini holat bilan XOR amalida qo‘shish va o‘zi o‘ziga teskari amal hisoblanadi.

```
def addRoundKey(state,roundkey):
        return state ^ roundkey
```

3.2. Ikkinchi akslantirish chiziqsiz S jadvali asosida amalga oshiriladi. Uning shifrlash va deshifrlash uchun ko‘rinishlari quyida keltirilgan.

```
def sBoxLayer(state):
        """SBox function for encryption

        Input:  64-bit integer
        Output: 64-bit integer"""

        output = 0
        for i in range(16):
                output += Sbox[( state >> (i*4)) & 0xF] << (i*4)
        return output
def sBoxLayer_dec(state):
        """Inverse SBox function for decryption

        Input:  64-bit integer
        Output: 64-bit integer"""
        output = 0
        for i in range(16):
                output += Sbox_inv[( state >> (i*4)) & 0xF] << (i*4)
        return output
```

3.3. Chiziqli P akslantirishni shifrlash va deshifrlash uchun ko‘rinishi quyida keltirilgan.

```
def pLayer(state):
        """Permutation layer for encryption

        Input:  64-bit integer
        Output: 64-bit integer"""
        output = 0
        for i in range(64):
                output += ((state >> i) & 0x01) << PBox[i]
        return output

def pLayer_dec(state):
        """Permutation layer for decryption

        Input:  64-bit integer
        Output: 64-bit integer"""
        output = 0
        for i in range(64):
                output += ((state >> i) & 0x01) << PBox_inv[i]
        return output
```

4. Python dasturida shifrni amalga oshirish uchun foydalanilgan qo‘shimcha funksiyalar.

4.1. Qatordan songa konvertatsiya qilish:

```
def string2number(i):
    """ Convert a string to a number

    Input: string (big-endian)
    Output: long or integer
    """

    val = int.from_bytes(i, byteorder='big')

    return val
```

4.2. Sondan qatorga konvertatsiya qilish:

```
def number2string_N(i, N):
    """Convert a number to a string of fixed size

    i: long or integer
    N: length of string
    Output: string (big-endian)
    """
    s = '%0*x' % (N*2, i)
    return binascii.unhexlify(str(s))
```

5. PRESENT shifrini Python dasturlash tilida (Present nomli) klass shaklida amalga oshirish.

5.1. Klass uchun konstruksiyani hosil qilish:

```
def __init__(self,key,rounds=32):
        """Create a PRESENT cipher object

        key:    the key as a 128-bit or 80-bit rawstring
        rounds: the number of rounds as an integer, 32 by default
        """
        self.rounds = rounds
        if len(key) * 8 == 80:
                self.roundkeys = generateRoundkeys80(string2number(key),self.rounds)
        elif len(key) * 8 == 128:
                self.roundkeys = generateRoundkeys128(string2number(key),self.rounds)
        else:
                raise ValueError("Key must be a 128-bit or 80-bit rawstring")
```

5.2. Shifrlash funksiyasi:

```
def encrypt(self,block):
        """Encrypt 1 block (8 bytes)

        Input:  plaintext block as raw string
        Output: ciphertext block as raw string
        """
        state = string2number(block)
        for i in range (self.rounds-1):
                state = addRoundKey(state,self.roundkeys[i])
                state = sBoxLayer(state)
                state = pLayer(state)
        cipher = addRoundKey(state,self.roundkeys[-1])
        return number2string_N(cipher,8)
```

5.3. Deshifrlash funksiyasi:

```
def decrypt(self,block):
        """Decrypt 1 block (8 bytes)

        Input:  ciphertext block as raw string
        Output: plaintext block as raw string
        """
        state = string2number(block)
        for i in range (self.rounds-1):
                state = addRoundKey(state,self.roundkeys[-i-1])
                state = pLayer_dec(state)
                state = sBoxLayer_dec(state)
        decipher = addRoundKey(state,self.roundkeys[0])
        return number2string_N(decipher,8)
```

5.4. Blok o‘lchamini olish:

```
def get_block_size(self):
        return 8
```

6. Present nomli klassdan ma’lumotni shifrlash va deshifrlashda foydalanish tartibi:

```
def _test():
    import Padding

    k="00000000000000000000"
    key = bytes.fromhex(k)
    cipher = Present(key)
    plaintext = "hello"
    text = Padding.appendPadding(plaintext,blocksize=8,mode='CMS')
    encrypted = cipher.encrypt(text.encode())
    print ('Cipher:\t\t'+encrypted.hex())
    decrypted = cipher.decrypt(encrypted)

    print ('Decrypted:\t'+decrypted.hex())
    print ('Decrypted:\t'+Padding.removePadding(decrypted.decode(),blocksize=8,mode='CMS'))
```

Ushbu funksiyani chaqirish tartibi:

```
if __name__ == "__main__":
    _test()
```

Amaliy bajarish uchun vazifalar

1. Yuqorida keltirilgan kodni batafsil o‘rgangan holda, uni bir ochiq matn bloki uchun shifrlash, deshifrlash, raund kalitlarini hosil qilish ketma-ketligini batafsil chop etuvchi sifatida o‘zgartiring.

2. Kiritilgan ochiq matn bloki uchun batafsil natijalarni chop eting va uni hisobotda aks ettiring.

3. Yuqorida keltirilgan kod uchun jarayon talab etgan vaqtni millisekundda hisoblang.

Adabiyot va Internet saytlar:

1. Bogdanov A. et al. PRESENT: An ultra-lightweight block cipher //Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. – Springer Berlin Heidelberg, 2007. – C. 450-466.

5. https://crypto.orange-labs.fr/papers/ches2007-450.pdf

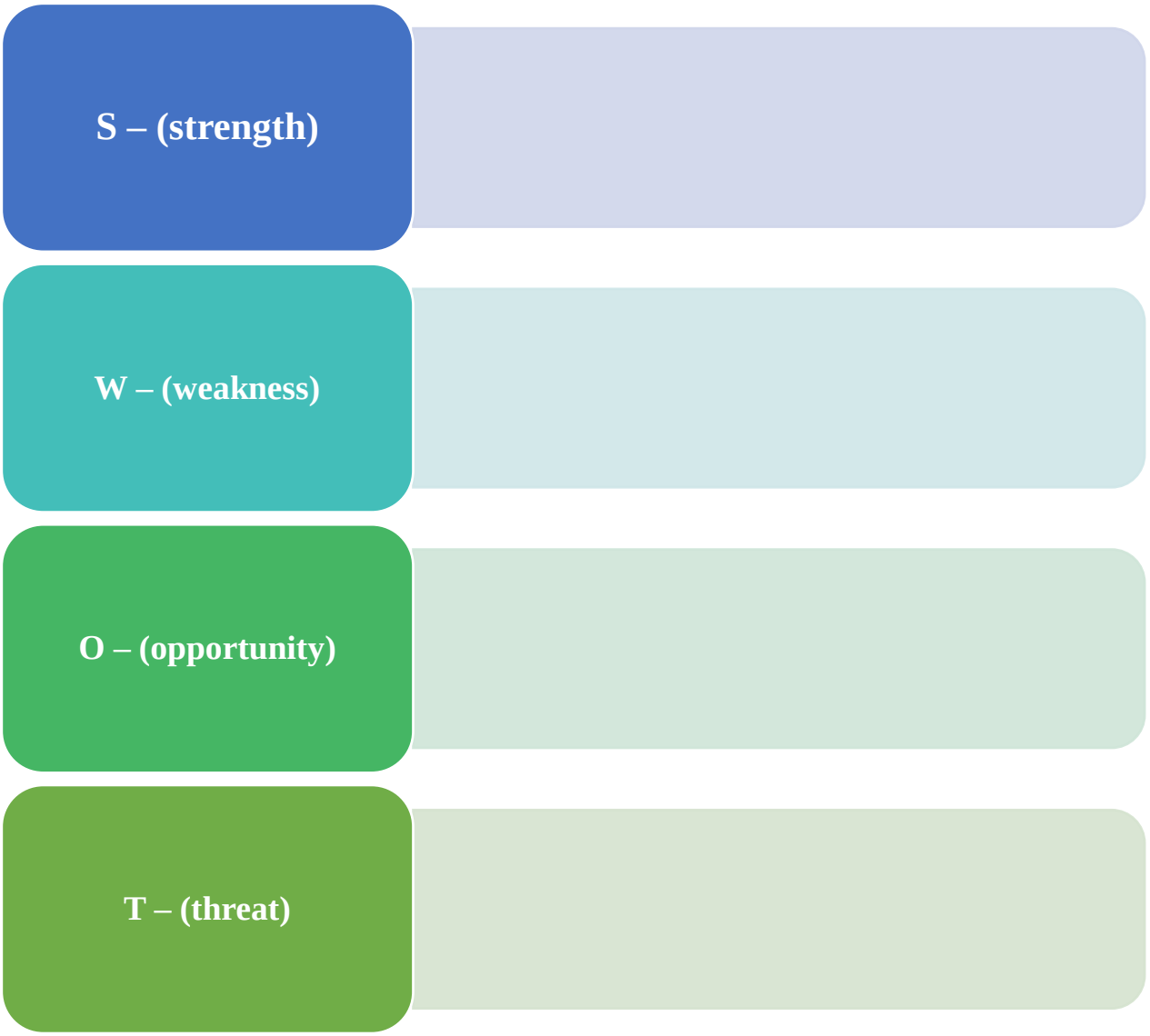
V-BO‘LIM.

KEYSLAR BANKI

V. KEYSLAR BANKI

1-keys mavzusi: SWOT tahlili usulidan foydalanib yengil vanzli shifrlash algoritmlarini tahlillash

Vaziyat tavsifi: yengil vaznli shifrlash algoritmlarini SWOT tahlil yordamida ularning, kuchli, zaif, imkoniyatlari va ularga qaratilgan tahdidlarni aniqlang.

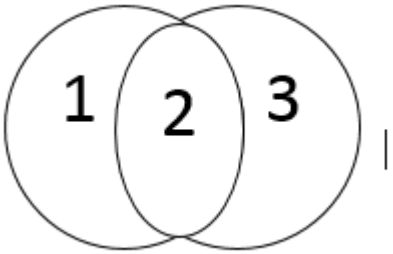


2-keys mavzusi: “Ananaviy va yengil vanzli kriptografik algoritmlarni taqqoslang”

Vaziyat tavsifi: Ananaviy va yengil vanzli kriptografik algoritmlarni taqqoslash orqali, afzallik va kamchiliklarni aniqlash.

Keys savollari:

1) Har ikkala turni o‘xshash va farqli tomonlarini o‘rganishda Ven diagrammasidan foydalaning?



2) Quyidagi jadvalni to‘lidirish orqali ularning afzallik va kamchiliklarini ayting?

№	Kriptografik algoritmlar	Afzalliklari	Kamchiliklari	Misollar
1	**Ananaviy kriptografiya**			
2	**Yengil vaznli kriptografiya**			

VI BO‘LIM.

GLOSSARIY

VI. GLOSSARIY

Tushuncha O‘zbek tilida	Tushunchaning o‘zbek tilidagi sharhi	Tushuncha ingliz tilida
kalitlar generatori	Kriptografik kalitlarni yoki initsializatsiya qilish vektorlarini ishlab chiqish uchun mo‘ljallangan apparat, apparat-dasturiy yoki dasturiy vosita	key generator
kriptografik bardoshlilik	Kriptografik tizimga (kriptografik mexanizm) bo‘ladigan hujumlarga dosh bera olish qobiliyatini tavsiflovchi kriptografik tizimning yoki alohida kriptografik mexanizmning xususiyati	cryptographic security
Protokol	1 Ikki yoki bir nechta mustaqil qurilmalar yoki jarayonlar o‘rtasida ma’lumotlar uzatish formati va tartibotini tartibga soluvchi qoidalar va kelishuvlar majmuasi. 2 Ma’lum bir natijaga erishish maqsadida ikki va undan ko‘p subyekt tomonidan berilgan ketma-ketlikda bajariladigan harakatlar (yo‘riqnomalar, buyruqlar, hisoblashlar, algoritmlar)ning majmuasi	protocol
yengil vaznli kriptografiya	Cheklangan muhitda amalga oshirish uchun moslashtirilgan kriptografiya	lightweight cryptography
elliptik egri chiziq	Chekli oddiy maydonda $y^2 = x^3 + ax + b$ tenglamasini qanoatlantiruvchi (x,y) nuqtalar to‘plami	elliptic curve
elektron raqamli imzo algoritmi	Himoyalanmagan umumiy foydalanishdagi telekommunikatsiya kanallari orqali uzatiladigan ma’lum bir xabar (elektron hujjat) ostidagi elektron raqamli imzoni shakllantirish va uning haqiqiyligini tasdiqlash uchun mo‘ljallangan kriptogrik algoritm.	electronic digital signature algorithm
asimmetrik shifrlash	Shifrlash va ochiq matnga o‘girish	asymmetric

	uchun turli kalitlar qo‘llaniladigan usul, ulardan birini boshqasining asosida hisoblab chiqarish murakkab	encryption
simmetrik kriptotizim (maxfiy kalitli kriptotizim)	Aynan bitta kriptografik kalitdan axborotni shifrlash va ochiq matnga o‘girish uchun foydalaniladigan kriptografik tizim	secret key crypto-system (symmetric cryptosystem)
operativ xotira xajmi	Kriptografik mexanizmni tasodifiy foydalana olish (kirish) xotirasida, shu jumladan protsessor registrlarida saqlash uchun vaqt maydoni	random access memory size
Kriptografiya	Axborot mazmunidan ruxsat etilmagan tarzda foydalanishdan muhofaza qilish, uni soxtalashtirish imkoniyatini yo‘qqa chiqarish maqsadida axborotni almashtirish prinsiplari, vositalari va usullarini o‘rganadigan ilmiy fan (bilimlar sohasidir).	Cryptography
Kriptologiya	Kriptografik almashtirishlarni o‘rganuvchi fan (bilimlar sohasi) bo‘lib, u ikki yo‘nalishni – kriptografiya va kriptotahlilni o‘z ichiga oladi.	Cryptology
kalit (kriptografik)	Kriptografik algoritm parametrlarining ma’lum bir to‘plamining o‘ziga xos maxfiy holati, ma’lum bir algoritm uchun mumkin bo‘lgan akslantirishlar (almashtirishlar) to‘plamidan bittasini tanlab olinishini ta’minlaydi. 2 Asimmetrik kriptotizimlar ochiq va maxfiy kalitlarining umumiy nomi: elektron raqamli imzoni hisoblash yoki tekshirish, shuningdek shifrlash va dastlab-ki matnga o‘girish uchun qo‘llaniladigan simvollar ketma-ketligidan iborat.	key (cryptographic)

VII BO‘LIM.

ADABIYOTLAR RO‘YXATI

VII. ADABIYOTLAR RO'YXATI

I. O‘zbekiston Respublikasi Prezidentining asarlari:

1. Mirziyoyev SH.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – T.: “O‘zbekiston”, 2017. – 488 b.

2. Mirziyoyev SH.M. Milliy taraqqiyot yo‘limizni qat’iyat bilan davom ettirib, yangi bosqichga ko‘taramiz. 1-jild. – T.: “O‘zbekiston”, 2017. – 592 b.

3. Mirziyoyev SH.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T.: “O‘zbekiston”, 2018. – 507 b.

4. Mirziyoyev SH.M. Niyati ulug‘ xalqning ishi ham ulug‘, hayoti yorug‘ va kelajagi farovon bo‘ladi. 3-jild.– T.: “O‘zbekiston”, 2019. – 400 b.

5. Mirziyoyev SH.M. Milliy tiklanishdan – milliy yuksalish sari. 4-jild.– T.: “O‘zbekiston”, 2020. – 400 b.

II. Normativ-huquqiy hujjatlar:

6. O‘zbekiston Respublikasining Konstitusiyasi.–T.:O‘zbekiston, 2018.

7. O‘zbekiston Respublikasining 2020-yil 23-sentabrda qabul qilingan “Ta’lim to‘g‘risida”gi O‘RQ-637-sonli Qonuni.

8. O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevral “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi 4947-sonli Farmoni.

9. O‘zbekiston Respublikasi Prezidentining 2018-yil 21-sentabr “2019-2021 yillarda O‘zbekiston Respublikasini innovatsion rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PF-5544-sonli Farmoni.

10. O‘zbekiston Respublikasi Prezidentining 2019-yil 27-may “O‘zbekiston Respublikasida korrupsiyaga qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PF-5729-son Farmoni.

11. O‘zbekiston Respublikasi Prezidentining 2019-yil 27-avgust “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to‘g‘risida”gi PF-5789-sonli Farmoni.

12. O‘zbekiston Respublikasi Prezidentining 2019-yil 8-oktabr “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030-yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5847-sonli Farmoni.

13. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-son Qarori.

14. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning 2020-yil 25-yanvardagi Oliy Majlisga Murojaatnomasi.

15. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2001-yil 16-avgustdagi “Oliy ta’limning davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi

343-sonli Qarori.

16. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015-yil 10-yanvardagi “Oliy ta’limning Davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi 2001-yil 16-avgustdagi “343-sonli qororiga o‘zgartirish va qo‘shimchalar kiritish haqida”gi 3-sonli qarori.

III. Maxsus adabiyotlar:

17. Cirani S. et al. Internet of things: architectures, protocols and standards. – John Wiley & Sons, 2018.

18. Akbarov D. Y. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008 – 394 bet.

IV. Internet saytlar:

19. http://edu.uz – O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi.

20. http://lex.uz – O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi.

21. http://bimm.uz – Oliy ta’lim tizimi pedagog va rahbar kadrlarini qayta tayyorlash va ularning malakasini oshirishni tashkil etish Bosh ilmiy-metodik markazi.

22. http://ziyonet.uz – Ta’lim portali ZiyonET.

23. http://natlib.uz – Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi.

24. https://csrc.nist.gov/projects/lightweight-cryptography - Lightweight Cryptography.