RESURSLARI CHEKLANGAN IoT QURILMALARI UCHUN YENGIL AUTENTIFIKATSIYALANGAN SHIFRLASH ALGORITMLARINING QIYOSIY TAHLILI

Mavlonova Shodmonoy Bog‘bek qizi
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
Axborot xavfsizligi kafedrasi o‘qituvchisi,
shodmonoy0906@gmail.com
Mavlonov Alisher Bagbekovich
Kriptologiya maktabi rahbari,
Axborot xavfsizligi va kriptologiya ilmiy-tadqiqot bo‘limi,
Unicon.uz mas’uliyati cheklangan jamiyati (MChJ) Toshkent, O‘zbekiston
mavlonosher@gmail.com

Annotatsiya. *Ushbu maqolada resurslari cheklangan Internet buyumlari (IoT) qurilmalarida ma’lumotlarni himoyalash uchun qo‘llaniladigan autentifikatsiyalangan shifrlash (AEAD) algoritmlari qiyosiy tahlil qilingan.*

2025-yil avgust oyida NIST tomonidan SP 800-232 standarti sifatida qabul qilingan Ascon-AEAD128 algoritmi an’anaviy AES-GCM va AES-CCM, ChaCha20-Poly1305 hamda PRESENT, SPECK va GIFT-COFB yengil algoritmlari bilan kriptografik xavfsizlik, tuzilma, dasturiy va apparat realizatsiya xarajatlari, yon kanal hujumlariga chidamlilik va standartlashtirilganlik mezonlari bo‘yicha solishtirilgan. Tahlil natijasida RFC 7228 hujjatidagi qurilma sinflari va turli foydalanish ssenariylari uchun algoritm tanlash bo‘yicha amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: *Internet buyumlari, yengil kriptografiya, Ascon, autentifikatsiyalangan shifrlash, AEAD, AES-GCM, ChaCha20-Poly1305, resurslari cheklangan qurilmalar.*

Аннотация. *В статье проведён сравнительный анализ алгоритмов аутентифицированного шифрования (AEAD), применяемых для защиты данных на устройствах Интернета вещей (IoT) с ограниченными ресурсами. Алгоритм Ascon-AEAD128, утверждённый NIST в августе 2025 года в качестве стандарта SP 800-232, сравнивается с традиционными алгоритмами AES-GCM и AES-CCM, ChaCha20-Poly1305, а также с лёгкими алгоритмами PRESENT, SPECK и GIFT-COFB по критериям*

криптостойкости, структуры, затрат на программную и аппаратную реализацию, устойчивости к атакам по сторонним каналам и статуса стандартизации. По результатам анализа сформулированы практические рекомендации по выбору алгоритма для классов устройств согласно RFC 7228 и типовых сценариев применения.

Ключевые слова: *Интернет вещей, лёгкая криптография, Ascon, аутентифицированное шифрование, AEAD, AES-GCM, ChaCha20-Poly1305, устройства с ограниченными ресурсами.*

Abstract. *This paper presents a comparative analysis of authenticated encryption (AEAD) algorithms used to protect data on resource-constrained Internet of Things (IoT) devices. Ascon-AEAD128, standardized by NIST in August 2025 as SP 800-232, is compared with the conventional AES-GCM and AES-CCM, ChaCha20-Poly1305, and the lightweight algorithms PRESENT, SPECK and GIFT-COFB with respect to security, structure, software and hardware implementation cost, side-channel resistance and standardization status. Based on the analysis, practical recommendations are given for selecting an algorithm for the device classes defined in RFC 7228 and for typical deployment scenarios.*

Keywords: *Internet of Things, lightweight cryptography, Ascon, authenticated encryption, AEAD, AES-GCM, ChaCha20-Poly1305, resource-constrained devices.*

1. Kirish

Internet buyumlari (IoT) texnologiyalari sanoat, sog‘liqni saqlash, qishloq xo‘jaligi, energetika va “aqlli shahar” tizimlarida keng qo‘llanilmoqda. Bunday tizimlarning asosini sensorlar, aktuatorlar, RFID teglar, aqlli hisoblagichlar va tibbiy implantlar kabi kichik qurilmalar tashkil etadi. Ularning aksariyati bir necha kilobayt operativ xotira, past chastotali mikrokontroller va cheklangan quvvat manbai (batareya) bilan ishlaydi. Shu bilan birga, bu qurilmalar orqali uzatiladigan ma’lumotlar (tibbiy ko‘rsatkichlar, boshqaruv buyruqlari, hisoblagich qiymatlari) maxfiylik va yaxlitlik nuqtai nazaridan muhim hisoblanadi.

An’anaviy kriptografik standartlar, jumladan AES va SHA-2, asosan shaxsiy kompyuter va serverlar uchun loyihalangan. Ular kichik qurilmalarda ham ishlashi mumkin, ammo kod hajmi, xotira sarfi, energiya iste’moli va yon kanal hujumlariga chidamlilik jihatidan har doim ham maqbul emas. Shu sababli

kriptografiyaning alohida yo‘nalishi - yengil kriptografiya (lightweight cryptography) shakllandi.

AQSh Milliy standartlar va texnologiyalar instituti (NIST) 2013-yildan boshlab cheklangan muhitlar uchun kriptografiyani o‘rganishni boshladi va 2018-yilda ochiq tanlov e’lon qildi. Tanlovga 57 ta algoritm taqdim etilgan, 2021-yilda

10 ta finalist aniqlangan va 2023-yil 7-fevralda Ascon algoritmlar oilasi g‘olib deb e’lon qilingan [2]. 2025-yil 13-avgustda Ascon asosidagi algoritmlar

NIST SP 800-232 standarti sifatida rasman nashr etildi [1].

Yangi standartning paydo bo‘lishi amaliy savolni yuzaga keltiradi: muayyan IoT qurilmasi uchun qaysi autentifikatsiyalangan shifrlash algoritmini tanlash maqsadga muvofiq? Ushbu maqolaning maqsadi Ascon-AEAD128 algoritmini keng tarqalgan an’anaviy va yengil algoritmlar bilan yagona mezonlar tizimi asosida qiyosiy tahlil qilish va qurilma sinflari bo‘yicha tavsiyalar ishlab chiqishdan iborat.

2. Resurslari cheklangan qurilmalar va ularga qo‘yiladigan talablar

IETF tashkilotining RFC 7228 hujjatida resurslari cheklangan qurilmalar xotira hajmiga ko‘ra uch sinfga ajratilgan [4] (1-jadval).

1-jadval

RFC 7228 bo‘yicha cheklangan qurilmalar sinflari

Sinf	Operativ xotira (RAM)	Doimiy xotira (Flash)	Tavsif
0-sinf (C0)	≪ 10 KiB	≪ 100 KiB	Odatda shlyuz orqali ishlaydi, to‘liq xavfsizlik protokollarini bajara olmaydi
1-sinf (C1)	~ 10 KiB	~ 100 KiB	CoAP kabi maxsus protokollar bilan ishlay oladi
2-sinf (C2)	~ 50 KiB	~ 250 KiB	Ko‘pgina standart protokollarni qo‘llay oladi

Bunday qurilmalar uchun kriptografik algoritmga quyidagi asosiy talablar qo‘yiladi: kichik kod hajmi va operativ xotira sarfi; bir bayt ma’lumotni qayta ishlash uchun kam energiya; apparat realizatsiyada kichik maydon (GE gate equivalent); yon kanal (vaqt, quvvat iste’moli) hujumlariga chidamlilik; maxfiylik va yaxlitlikni bitta amalda ta’minlovchi AEAD rejimining mavjudligi; nonce va autentifikatsiya tegi (tag) hisobiga qo‘shiladigan qo‘shimcha baytlarning kamligi. Oxirgi talab ayniqsa muhim, chunki, masalan, IEEE 802.15.4 tarmoqlarida bitta freym hajmi 127 bayt bilan cheklangan.

3. Tadqiqot metodikasi

Tadqiqot analitik-qiyosiy usulda olib borildi. Manba sifatida algoritmlarning rasmiy spetsifikatsiyalari va standartlari [1, 5–13], NIST tanlovining yakuniy hisoboti [2] hamda mikrokontrollerlarda o‘tkazilgan ochiq benchmark natijalari

[14, 15] tahlil qilindi. Algoritmlar quyidagi oltita mezon bo‘yicha baholandi:

K1 - kriptografik xavfsizlik darajasi (kalit va teg uzunligi, xavfsizlik zaxirasi, ma’lum kriptotahlil natijalari);

K2 - apparat tezlatkichisiz mikrokontrollerlarda dasturiy samaradorlik;

K3 - apparat realizatsiya xarajati (maydon, energiya);

K4 - yon kanal hujumlariga chidamlilik va himoya choralarini (maskalash) qo‘llash qulayligi;

K5 - funksional universallik (AEAD, xesh, XOF funksiyalarini bitta yadro asosida qurish imkoniyati);

K6 - standartlashtirilganlik va IoT protokollarida qo‘llab-quvvatlanishi.

Har bir mezon bo‘yicha baho “yuqori”, “o‘rta” yoki “past” darajada, adabiyotlardagi ma’lumotlarni umumlashtirish asosida berildi.

4. Tahlil qilinayotgan algoritmlar tavsifi

AES-GCM va AES-CCM. AES (FIPS 197) 128 bitli blokli, SPN tuzilmali shifr bo‘lib, 128 bitli kalit uchun 10 raunddan iborat [5]. GCM rejimi (SP 800-38D) hisoblagich rejimida shifrlash va GF(2^{128}) maydonida ko‘paytirishga asoslangan GHASH autentifikatsiyasini birlashtiradi [6]. CCM rejimi (SP 800-38C) hisoblagich rejimi va CBC-MAC ga asoslangan bo‘lib, faqat AES ning shifrlash funksiyasini talab qiladi [7]. AES-CCM IEEE 802.15.4, Bluetooth Low Energy va Zigbee texnologiyalarida qo‘llaniladi, OSCORE protokolida esa AES-CCM-16-64-128 standart algoritm sifatida belgilangan [12]. AES ning asosiy afzalligi, ko‘plab zamonaviy mikrokontrollerlarda apparat tezlatkichning mavjudligi. Kamchiliklari: jadvalli dasturiy realizatsiyalar kesh-vaqt hujumlariga zaif [17]; GHASH apparat qo‘llovisiz qimmat amal; GCM da nonce qayta ishlatilsa, autentifikatsiya kaliti tiklanishi mumkin [16].

ChaCha20-Poly1305. RFC 8439 da standartlashtirilgan bu sxema 256 bitli kalit, 96 bitli nonce va 128 bitli tegdan foydalanadi [8]. ChaCha20 oqimli shifri 512 bitli holat ustida 20 raund ARX (qo‘shish, siklik siljitish, XOR) amallarini bajaradi. ARX amallari tabiiy ravishda doimiy vaqtda bajariladi, bu vaqt bo‘yicha yon kanal hujumlariga chidamlilikni ta’minlaydi. Algoritm 32 bitli protsessorlarda apparat tezlatkichisiz ham samarali ishlaydi va TLS 1.3 da keng

qo‘llaniladi. Biroq Poly1305 ning 130 bitli arifmetikasi 8 bitli mikrokontrollerlarda nisbatan og‘ir hisoblanadi.

Ascon. Ascon C. Dobraunig, M. Eichlseder, F. Mendel va M. Schläffer tomonidan ishlab chiqilgan [3]. U 2019-yilda CAESAR tanlovida yengil qo‘llanmalar uchun birinchi tanlov sifatida e’tirof etilgan va NIST tanlovida g‘olib bo‘lgan. Ascon gubka (duplex) konstruksiyasiga asoslanadi: beshta 64 bitli so‘zdan iborat 320 bitli ichki holat ustida konstanta qo‘shish, 5 bitli S-blok (bitslice usulida) va chiziqli diffuziya qatlamlaridan tashkil topgan permutatsiya qo‘llaniladi. SP 800-232 standartida to‘rtta funksiya belgilangan: Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128 va Ascon-CXOF128 [1]. Ascon-AEAD128 da kalit, nonce va teg uzunligi 128 bitni tashkil etadi; initsializatsiya va yakunlashda 12 raundli, ma’lumotlarni qayta ishlashda 8 raundli permutatsiya ishlatiladi. Bitta permutatsiya asosida shifrlash, xeshlash va XOF funksiyalarini amalga oshirish mumkinligi umumiy kod hajmini kamaytiradi. Bitslice S-blok doimiy vaqtli realizatsiyani va maskalash orqali yon kanal himoyasini qulaylashtiradi [15].

PRESENT. 2007-yilda taklif etilgan, 64 bitli blokli, 80 yoki 128 bitli kalitli, 31 raundli SPN shifr [9]. U 4 bitli S-blok va bit o‘rin almashtirishdan foydalanadi, ISO/IEC 29192-2 standartiga kiritilgan [13]. Apparat realizatsiyada juda kichik maydon talab qiladi, ammo bit o‘rin almashtirish tufayli dasturiy realizatsiyada sekin. 64 bitli blok uzunligi bitta kalit bilan xavfsiz shifrlanadigan ma’lumot hajmini cheklaydi. AEAD sifatida ishlatish uchun qo‘shimcha rejim talab qilinadi.

SPECK. 2013-yilda AQSh Milliy xavfsizlik agentligi (NSA) tomonidan e’lon qilingan ARX tuzilmali blokli shifrlar oilasi [10]. Dasturiy realizatsiyada juda ixcham va tez. Biroq loyihalash asoslarining yetarlicha ochiqlanmaganligi sababli 2018-yilda ISO standartlashtirishdan rad etilgan, bu esa unga bo‘lgan ishonchni pasaytiradi.

GIFT-COFB. GIFT shifri (2017) PRESENT tuzilmasini takomillashtirish natijasida yaratilgan [11]. GIFT-128 asosidagi GIFT-COFB AEAD sxemasi NIST tanlovining finalistlaridan biri bo‘lgan, biroq standart sifatida tanlanmagan [2].

5. Qiyosiy tahlil natijalari

Algoritmlarning asosiy parametrlari 2-jadvalda keltirilgan.

2-jadval

Algoritmlarning asosiy parametrlari

Algoritm	Tuzilma	Kalit, bit	Blok / holat, bit	Nonce, bit	Teg, bit	Raund	Standart
AES-128-GCM	SPN + GHASH	128	128	96	128	10	FIPS 197, SP 800-38D
AES-128-CCM	SPN + CBC-MAC	128	128	56–104	32–128	10	SP 800-38C
ChaCha20-Poly1305	ARX + Poly1305	256	512	96	128	20	RFC 8439
Ascon-AEAD128	Gubka (duplex)	128	320	128	128	12 / 8	NIST SP 800-232
PRESENT	SPN	80 / 128	64	—*	—*	31	ISO/IEC 29192-2
SPECK-64/128	ARX	128	64	—*	—*	27	—
GIFT-COFB	SPN + COFB	128	128	128	128	40	NIST finalisti

** Blokli shifr; AEAD uchun alohida ishlash rejimi talab etiladi.*

Belgilangan mezonlar bo‘yicha sifat baholash natijalari 3-jadvalda umumlashtirilgan.

3-jadval

Algoritmlarni mezonlar bo‘yicha qiyosiy baholash

Algoritm	K1	K2	K3	K4	K5	K6
AES-GCM / CCM	Yuqori	O‘rta	O‘rta	Past–o‘rta	Past	Juda yuqori
ChaCha20-Poly1305	Yuqori	Yuqori	Past	O‘rta	Past	Yuqori
Ascon-AEAD128	Yuqori	Yuqori	Yuqori	Yuqori	Yuqori	O‘sib bormoqda
PRESENT	O‘rta	Past	Juda yuqori	O‘rta	Past	O‘rta
SPECK	O‘rta	Yuqori	Yuqori	O‘rta	Past	Past
GIFT-COFB	Yuqori	O‘rta	Yuqori	O‘rta	Past	Past

Tahlil natijalarini quyidagicha izohlash mumkin. Birinchidan, xavfsizlik (K1) bo‘yicha AES, ChaCha20-Poly1305 va Ascon zamonaviy talablarga to‘liq javob beradi. NIST yakuniy hisobotida Ascon ning tanlanishiga yuqori xavfsizlik zaxirasi va mustaqil tadqiqotchilar tomonidan o‘tkazilgan katta hajmdagi kriptotahlil asos bo‘lgani qayd etilgan [2]. PRESENT va SPECK ning 64 bitli blok uzunligi esa uzoq muddatli foydalanishda cheklov hisoblanadi.

Ikkinchidan, apparat tezlatkichisiz mikrokontrollerlarda (K2) Ascon va ChaCha20-Poly1305 eng yaxshi natijalarni ko‘rsatadi. Ochiq benchmarklarda 8 bitli AVR mikrokontrollerida NIST finalistlari AES-GCM bilan solishtirilganda, Ascon tezlik bo‘yicha finalistlar orasida yuqori o‘rinlardan birini egallagan va GIFT-COFB dan oldinda bo‘lgan [14]. Shu bilan birga, mikrokontrollerda AES apparat bloki mavjud bo‘lsa, AES-CCM tezlik va energiya bo‘yicha eng samarali variant bo‘lib qoladi.

Uchinchidan, yon kanal hujumlariga chidamlilik (K4) va funksional universallik (K5) bo‘yicha Ascon ustunlikka ega: bitslice tuzilma maskalashni qulaylashtiradi, yagona permutatsiya esa AEAD, xesh va XOF funksiyalarini kichik kod hajmida amalga oshirish imkonini beradi. AES va ChaCha20-Poly1305 bilan xeshlash uchun alohida algoritm (masalan, SHA-256) qo‘shilishi kerak.

To‘rtinchidan, standartlashtirilganlik va ekotizim (K6) bo‘yicha AES hozircha raqobatsiz: u mavjud IoT protokollarining deyarli barchasida qo‘llaniladi. Ascon esa yangi standart bo‘lib, uni IoT protokollariga (masalan, COSE/OSCORE) integratsiya qilish ishlari endi boshlanmoqda.

6. Algoritm tanlash bo‘yicha tavsiyalar

Olingan natijalar asosida turli ssenariylar uchun tavsiyalar 4-jadvalda keltirilgan.

4-jadval

Foydalanish ssenariylari bo‘yicha tavsiyalar

Ssenariy	Tavsiya etilgan algoritm	Asosiy sabab
0-sinf qurilmalar, RFID teglar, maxsus mikrosxemalar (ASIC)	Ascon-AEAD128	Kichik apparat maydoni, AEAD va xesh bitta yadroda
1–2-sinf mikrokontrollerlar, AES apparat tezlatkichi mavjud	AES-CCM	Apparat tezlashtirish, protokollar bilan moslik

Ssenariy	Tavsiya etilgan algoritm	Asosiy sabab
1–2-sinf mikrokontrollerlar, apparat tezlatkichisiz	Ascon-AEAD128	Yuqori dasturiy samaradorlik, kichik kod hajmi
2-sinf 32 bitli qurilmalar, TLS/DTLS bilan moslik talab etiladi	ChaCha20-Poly1305	Keng qo‘llab-quvvatlash, doimiy vaqtli realizatsiya
Qurilmaga jismoniy kirish xavfi yuqori (yon kanal hujumlari)	Ascon-AEAD128 (maskalash bilan)	Maskalash xarajatining nisbatan pastligi
Mavjud tizimlar bilan moslik (eski qurilmalar)	PRESENT / AES	Faqat yangi loyihalarda tavsiya etilmaydi

Algoritm tanlashdan qat’i nazar, quyidagi umumiy qoidalarga rioya qilish zarur: har bir kalit uchun nonce qiymatlari takrorlanmasligi kerak (bu ayniqsa AES-GCM uchun muhim); autentifikatsiya tegini qisqartirish faqat xavf darajasi asoslangan holda qo‘llanilishi lozim; kalitlarni boshqarish va almashinuv mexanizmlari alohida ishonchli protokol orqali ta’minlanishi kerak.

7. Xulosa

Maqolada resurslari cheklangan IoT qurilmalari uchun oltita autentifikatsiyalangan shifrlash yechimi oltita mezon bo‘yicha qiyosiy tahlil qilindi. Tahlil natijalari barcha holatlar uchun yagona eng yaxshi algoritm mavjud emasligini ko‘rsatdi. AES apparat tezlatkichi mavjud qurilmalarda va mavjud protokollar bilan moslik talab etilganda AES-CCM maqbul tanlov bo‘lib qoladi. Apparat tezlatkichisiz mikrokontrollerlar, juda kichik apparat qurilmalar va yon kanal hujumlari xavfi yuqori bo‘lgan muhitlar uchun esa NIST SP 800-232 standartidagi Ascon-AEAD128 eng muvozanatli yechim hisoblanadi. PRESENT va SPECK algoritmlarini yangi loyihalarda qo‘llash tavsiya etilmaydi.

Keyingi tadqiqotlar yo‘nalishi sifatida algoritmlarni mikrokontroller emulyatorlari va masofaviy test platformalarida amaliy o‘lchash, Ascon ni COSE/OSCORE protokollariga integratsiya qilish hamda yengil simmetrik kriptografiyani postkvant kalit almashinuvi protokollari bilan birgalikda qo‘llash masalalari belgilandi.

Foydalanilgan adabiyotlar

1. NIST SP 800-232. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. – Gaithersburg: NIST, 2025. – URL: https://csrc.nist.gov/pubs/sp/800/232/final

2. Sönmez Turan M., McKay K., Chang D. et al. Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process. NIST IR 8454. – NIST, 2023. – DOI: 10.6028/NIST.IR.8454

3. Dobraunig C., Eichlseder M., Mendel F., Schläffer M. Ascon v1.2: Lightweight Authenticated Encryption and Hashing // Journal of Cryptology. – 2021. – Vol. 34. – Art. 33.

4. Bormann C., Ersue M., Keranen A. Terminology for Constrained-Node Networks. RFC 7228. – IETF, 2014.

5. FIPS 197. Advanced Encryption Standard (AES). – NIST, 2001 (yangilangan 2023).

6. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. – NIST, 2007.

7. Dworkin M. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST SP 800-38C. – NIST, 2004.

8. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. – IETF, 2018.

9. Bogdanov A., Knudsen L.R., Leander G. et al. PRESENT: An Ultra-Lightweight Block Cipher // CHES 2007. LNCS. – Vol. 4727. – Springer, 2007. – P. 450–466.

10. Beaulieu R., Shors D., Smith J. et al. The SIMON and SPECK Families of Lightweight Block Ciphers. – IACR Cryptology ePrint Archive, 2013/404.

11. Banik S., Pandey S.K., Peyrin T. et al. GIFT: A Small Present // CHES 2017. LNCS. – Vol. 10529. – Springer, 2017. – P. 321–345.

12. Selander G., Mattsson J., Palombini F., Seitz L. Object Security for Constrained RESTful Environments (OSCORE). RFC 8613. – IETF, 2019.

13. ISO/IEC 29192-2:2019. Information security – Lightweight cryptography – Part 2: Block ciphers.

14. Weatherley R. Lightweight Cryptography Primitives: performance results of the NIST LWC finalists on embedded platforms. – URL: https://github.com/rweather/lightweight-crypto

15. Adomnicai A., Fournier J.J.A., Masson L. Masking the Lightweight Authenticated Ciphers ACORN and Ascon in Software. – IACR Cryptology ePrint Archive, 2018/708.

16. Joux A. Authentication Failures in NIST Version of GCM. – Comments submitted to NIST, 2006.

17. Bernstein D.J. Cache-timing attacks on AES. – Technical report, 2005.