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

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

2026-yil 25-26-sentabr

(2-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2026-yil 25-26-sentabr. 315-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., т.f.f.d.(PhD), dots. Abdumalikov A.A, p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O‘ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

µA (xi) va µA (xj) taqqoslash	Mij
µA (xi) teng µA (xj)	1
µA (xi) biroz katta µA (xj)	3
µA (xi) katta µA (xj)	5
µA (xi) sezilarli darajada katta µA (xj)	7
µA (xi) biroz katta µA (xj)	9
Yuqorida berilgan sonlar oralig‘idagi qiymatlar	2,4,6,8

Matritsaning diagonali bo‘yicha nosimmetrik elementlar quyidagi talabga javob berishi zarur.

$$a_{ij} = \frac{1}{a_{ij}}$$

Xulosa sifatida shuni aytish mumkinki noravshan to‘plam nazariyasi asosida inson yuzlarini tanib olishda usullarni to‘g‘ri tanlab olish kerakligi o‘rganildi. Maqolada bu usullarning to‘g‘ridan -to‘g‘ri va aylanma usullari keltirib o‘tildi. Birinchi usul sodda bo‘lsada, kutilgan natijani bermadi. Ikkinchi aylanma usul esa murakkabroq bo‘lib, biz kutgan samarali natijani beradi. Ushbu maqolada berilgan noravshan to‘plamlar nazariyasining asoslari va bilimlar bazasi kelajakda kadrlar uchun nafaqat o‘quv jarayonida, balki ularning kelajakdagi amaliy faoliyati uchun ham foydali bo‘ladi.

FOYDALANILGAN ADABIYOTLAR:

1. Мухамедова Д.Т. ―Норавшан ахборотни қайта ишлаш асосида суст шаклланган жараѐнларни башоратлаш ва муқобиллаштириш моделлари.‖ Тошкент.: ―Фан ва технология‖, 2012.- 376 бет.

2. Борисов В. В. Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. М.: Горячая линия — Телеком, 2007. 283 бет.

3. Ухоботов В. И. Введение в теорию нечетких множеств и ее приложения: ўқув қўлланма / В. И. Ухоботов. Челябинск: УрСЭИ АТ и СО, 2005. 133 бет.

4. https://cyberleninka.runoravshan-mantiq-nazariyasi-va-xususiyatlari.

IoT QURILMALARI UCHUN ELLIPTIK EGRI CHIZIQLARGA ASOSLANGAN YENGIL AUTENTIFIKATSIYA PROTOKOLINI ISHLAB CHIQISH MASALALARI

Qurbonova Mahzuna Ro‘ziboyevna,
Mirzo Ulug’bek nomidagi O‘zbekiston Milliy universitetining,
Axborot xavfsizligi kafedrasi, 05.01.02-Tizimli tahlil, boshqaruv va axborotlarni qayta ishlash” mutaxassisligi tayanch-doktoranti (PhD);
E-mail: mahzuna1214@icloud.com

Annotatsiya: Ushbu tezisda “narsalar internet” (Internet of Things) tarmoqlariga xos resurs cheklovlari - cheklangan xotira, past energiya sig’imi va past

hisoblash quvvati - sharoitida qurilmalar o’rtasida xavfsiz autentifikatsiyani ta’minlash masalasi ko’rib chiqiladi. An’anaviy ochiq kalitli kriptografik sxemalarning (xususan, RSA) IoT muhitida qo’llanilishidagi cheklovlar tahlil qilinadi, elliptik egri chiziqlar kriptografiyasiga (ECC) asoslangan yengillashtirilgan autentifikatsiya protokolining asosiy tamoyillari taklif etiladi.

Kalit so’zlar: IoT, elliptik egri chiziqlar kriptografiyasi, yengil kriptografiya, autentifikatsiya, resurs cheklangan qurilmalar.

Kirish

So’nggi yillarda narsalar interneti texnologiyalari jadal sur’atlarda rivojlanmoqda: sanoat sensorlari, aqlli uy qurilmalari, tibbiy monitoring vositalari va boshqa millionlab kichik qurilmalar bir-biri bilan doimiy ravishda ma’lumot almashmoqda. Bunday qurilmalarning aksariyati juda cheklangan resurslarga ega: RFC 7228 tasnifiga ko’ra, ularning operativ xotirasi bir necha kilobayt (ba’zan bir necha o’n kilobayt) atrofida, quvvat manbai esa ko’pincha kichik batareyadan iborat bo’ladi [1].

Bunday sharoitda klassik ochiq kalitli kriptografiya, xususan RSA algoritmi, amaliy jihatdan og’ir hisoblanadi. NIST tavsiyalariga ko’ra, taxminan 128 bitli xavfsizlik darajasini ta’minlash uchun RSA 3072 bitli modul talab qiladi, ECC esa atigi 256 bitli kalit bilan shu darajaga erishadi [2]. Kalit uzunligining bunday farqi nafaqat xotira sarfida, balki hisoblash murakkabligida ham sezilarli farqni keltirib chiqaradi: RSA’ning maxfiy kalit bilan bajariladigan amallari (imzolash, deshifrlash) va kalit generatsiyasi katta modul bo’yicha darajaga ko’tarishga asoslangan bo’lib, kichik mikrokontrollerlarda ECC ning skalyar ko’paytirishiga nisbatan ancha ko’p protsessor tsiklini talab qiladi [3].

Shuning uchun IoT qurilmalari uchun mo’ljallangan, yengillashtirilgan (lightweight) elliptik egri chiziqli autentifikatsiya mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy vazifa hisoblanadi.

Asosiy qism

Autentifikatsiya protokoli ishlab chiqilayotganda hisoblash murakkabligi, xotira sarfi va energiya iste’moli kabi mezonlar inobatga olinadi; ayni paytda resurslarni tejash xavfsizlik darajasini pasaytirmasligi shart.

1. Egri chiziq va maydon tanlovi. Yengil ECC sxemalarida odatda nisbatan qisqa kalitli egri chiziqlar tanlanadi: 8-bitli mikrokontrollerlardagi klassik tadqiqotlar 160-224 bitli NIST/SECG egri chiziqlariga tayangan [3]. Biroq kalit uzunligini qisqartirish xavfsizlik darajasini ham pasaytiradi: P-192 taxminan 96 bitli, P-224 esa 112 bitli xavfsizlik beradi [2]. Shu sababli P-192 NIST talab qiladigan 112 bitlik minimal darajaga yetmaydi, P-224 esa faqat qisqa muddatli ilovalar uchun mos keladi. Uzoq muddat ishlatiladigan qurilmalar uchun 128 bitli xavfsizlik beruvchi P-256 yoki Curve25519 maqsadga muvofiq. Curve25519 - Montgomery ko’rinishidagi zamonaviy egri chiziq bo’lib [4], NIST SP 800-186 (2023) hujjatida ham keltirilgan [5]. Uning afzalligi shundaki, X25519 funksiyasida skalyar ko’paytirish faqat x-koordinata ustida, doimiy vaqt (constant-time) rejimida bajarilishi mumkin; bu vaqt asosidagi yon kanal hujumlariga (timing attack) qarshilikni oshiradi. Skalyarni qayta ishlash qoidalari RFC 7748 da belgilangan [6].

2. Skalyar ko'paytirish algoritmi. Autentifikatsiya protokolining asosiy hisoblash yuki skalyar ko'paytirish amaliga ($k \cdot Q$, bunda k- skalyar, Q - egri chiziq nuqtasi) to'g'ri keladi [7]. Resurs cheklangan qurilmalarda bu amalni bajarish uchun Montgomery narvoni (Montgomery ladder) usuli tavsiya etiladi: u skalyarning har bir bitini bir xil tuzilishdagi ikkita amal (nuqtalarni qo'shish va ikkilantirish) bilan qayta ishlaydi, bu esa oddiy quvvat tahlili (SPA) va vaqt hujumlariga chidamlilikni oshiradi hamda kod hajmini ixchamlashtiradi. Shu bilan birga, narvonning o'zi doimiy vaqtni kafolatlamaydi: shartli almashtirish va maydon amallari ham doimiy vaqtda bajarilishi kerak. Sensor tarmoqlari uchun sozlanadigan ECC kutubxonasi TinyECC shu yo'nalishdagi amaliy misollardan biridir [8].

Taqqoslash uchun: 8 MGts li ATmega 128 mikrokontrollerida 160 bitli ECC skalyar ko'paytirishi taxminan 0,81 s vaqt oladi, RSA-1024 ning maxfiy kalit bilan amali esa taxminan 11 s ni tashkil etadi (kichik ochiq daraja ko'rsatkichli ochiq kalit amali - 0,43 s) [3]. Bu ikki usul taxminan 80 bitli xavfsizlik darajasiga mos keladi. 128 bitli daraja uchun esa X25519 shu turdagi mikrokontrollerda taxminan 13,9 mln tsikl talab qiladi [9], ya'ni xavfsizlik darajasi oshgani sayin hisoblash yuki ham ortadi va muvozanatni ehtiyotkorlik bilan tanlash zarur.

3. Autentifikatsiya sxemasi. Taklif etilayotgan protokol ikki tomonlama (mutual) autentifikatsiyani ECDH (Elliptic Curve Diffie-Hellman) kalit almashinuvi asosida quradi. Shuni ta'kidlash zarurki, ECDH o'zi faqat umumiy kalit kelishuvini ta'minlaydi, autentifikatsiyani esa kafolatlamaydi: ochiq nuqtalar tasdiqlanmagan holda almashilsa, "o'rtadagi odam" (man-in-the-middle) hujumi mumkin. Shu sababli protokolda quyidagilar nazarda tutiladi: a) har bir qurilmaning uzoq muddatli (statik) ochiq kaliti ro'yxatdan o'tkazish bosqichida ishonchli tugun (masalan, shlyuz) orqali qurilma identifikatoriga bog'lanadi; b) har bir seans uchun vaqtinchalik (ephemeral) kalit jufti hosil qilinib, statik va vaqtinchalik kalitlar bo'yicha ECDH natijalari birlashtiriladi, bu oldinga maxfiylikni (forward secrecy) ta'minlaydi; d) takroriy yuborish (replay) hujumlaridan himoya qilish uchun tasodifiy son (nonce) yoki hisoblagich ishlatiladi; e) qabul qilingan nuqtaning egri chiziqqa tegishliligi tekshiriladi [10] (Curve25519 da bu xavf skalyarni me'yorlashtirish (clamping) orqali kamayadi [6]); f) umumiy sirdan seans kalitlari xesh funksiyasi yordamida hosil qilinadi va tomonlar kalitni MAC orqali o'zaro tasdiqlaydi.

Xesh funksiyasi sifatida SHA-256 ning qisqartirilgan varianti o'rniga NIST tomonidan yengil kriptografiya uchun tanlangan Ascon oilasidan foydalanish maqsadga muvofiq: qisqartirish faqat chiqish uzunligini kamaytiradi, hisoblash va kod hajmini emas [11]. Bunday yondashuv to'liq sertifikatlarga asoslangan og'ir infratuzilmani talab qilmaydi, bu esa uni resurslari cheklangan IoT tarmoqlari uchun qulay qiladi.

1-jadvalda RSA va ECC asosidagi yondashuvlarning taxminiy taqqoslanishi keltirilgan.

1-jadval. RSA va ECC yondashuvlarining taxminiy taqqoslanishi [2, 3]

Mezon	**RSA-3072**	**ECC-256**
Xavfsizlik darajasi	~128 bit	~128 bit

Kalit uzunligi	3072 bit (modul)	256 bit
Xotira sarfi	Yuqori	Past
Hisoblash tezligi (kichik qurilmada, maxfiy kalit amali)	Sekin	Tezroq

Xulosa

O’tkazilgan tahlil IoT qurilmalarining apparat cheklovlari sharoitida klassik ochiq kalitli algoritmlarni (birinchi navbatda RSA ni) to’g’ridan-to’g’ri qo’llash amaliy jihatdan maqsadga muvofiq emasligini ko’rsatadi. Curve25519 kabi zamonaviy egri chiziqlar, Montgomery narvoni usuli va statik hamda vaqtinchalik kalitlarga asoslangan ECDH protokoli talab qilinadigan xavfsizlik darajasini saqlagan holda xotira, energiya va hisoblash resurslarini tejash imkonini beradi. Kelgusi tadqiqotlarda ushbu protokolni real 8/32-bitli mikrokontrollerlarda dasturiy amalga oshirish, uning xotira hajmi va energiya sarfini eksperimental o’lchash hamda rasmiy xavfsizlik tahlilini o’tkazish rejalashtirilgan.

Foydalanilgan adabiyotlar

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

2. Barker E. NIST Special Publication 800-57 Part 1 Rev. 5: Recommendation for Key Management. - NIST, 2020.

3. Gura N., Patel A., Wander A., Eberle H., Shantz S.C. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs // CHES 2004, LNCS 3156. - Springer, 2004. - P. 119 - 132.

4. Bernstein D.J. Curve25519: New Diffie-Hellman Speed Records // PKC 2006, LNCS 3958. - Springer, 2006. - P. 207–228.

5. Chen L. et al. NIST Special Publication 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. - NIST, 2023.

6. Langley A., Hamburg M., Turner S. RFC 7748: Elliptic Curves for Security. - IETF, 2016.

7. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. -Springer, 2004.

8. Liu A., Ning P. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks // IPSN 2008. - IEEE, 2008. - P. 245-256.

9. Düll M. et al. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers // Designs, Codes and Cryptography. - 2015. - Vol. 77. - P. 493–514.

10. Bos J.W. et al. Elliptic Curve Cryptography in Practice // Financial Cryptography and Data Security 2014, LNCS 8437. - Springer, 2014. - P. 157-175.

11. NIST Special Publication 800-232: Ascon-Based Lightweight Cryptography Standards for Constrained Devices. - NIST, 2025.