ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2023

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-3, ISSUE-5

ANALYSIS OF CRYPTOSYSTEMS BASED ON ELLIPTIC CURVES

Umarov Shohzod Zafar o‘g‘li
TUIT named after Muhammad al-Khorazmi, graduate student

Abstract – Elliptic Curve Cryptography (EECH) is a public-key cryptographic technique that uses the mathematical properties of elliptic curves to secure data transmission over the Internet. EECH is known for providing robust security, providing sufficient tolerance for smaller key lengths compared to traditional cryptographic methods such as RSA or Diffie-Hellman. In general, EECH is relevant in scenarios where security is important and computing resources are limited. This article presents an analysis of various cryptographic algorithms based on EECH.

Keywords - Elliptic curves, encryption algorithms, digital signature algorithms, key distribution algorithms

ELLIPTIK EGRI CHIZIQLARGA ASOSLANGAN KRIPTOTIZIMLAR TAHLILI

Umarov Shohzod Zafar o‘g‘li (*Muhammad al-Xorazmiy nomidagi TATU, magistrant*)

Annotatsiya – Elliptik egri chiziqlarga asoslangan kriptografiya (EECH) - bu Internet orqali ma'lumotlarni uzatishni himoya qilish uchun elliptik egri chiziqlarning matematik xususiyatlaridan foydalanadigan ochiq kalitli kriptografik usul hisoblanadi. EECH ishonchli himoyani ta'minlash bilan mashhur bo'lib, RSA yoki Diffie-Hellman kabi an'anaviy kriptografik usullariga nisbatan kichikroq kalit uzuligida ham yetarli bardoshlikni ta’minlab beradi. Umuman olganda, EECH xavfsizlik muhim bo'lgan va hisoblash resurslari cheklangan stsenariylarda dolzarbdir. Ushbu maqolada EECH asoslangan turli kriptgrafik algoritmlar tahlili keltirilgan.

Kalit so‘zlar – Elliptik egri chiziqlar, shiflrash algoritmlari, elektron raqamli imzo algoritmlari, kalitlarni taqsimlash algoritmlari

Ochiq kalitli kriptografiyaning barcha zamonaviy dizaynlari tizimlar xavfsizligini ta'minlash uchun guruh nazariyasiga tayanadi. EECH ning kriptografik bardoshliligi diskret logarifm muammosining murakkabligiga tayanadi. Xavfsizlik protokollari bilan bog‘langan ushbu tushuncha kalitlarni o‘rnatish, shifrlash, autentifikatsiyalash va imzolash xizmatlarini taqdim etish uchun ishlatilishi mumkin. Egri chiziqlar operatsiyalarida kirishlar elliptik egri chiziqdagi nuqtalar bo‘lib, ular elliptik egri chiziqning boshqa nuqtalarini topish uchun ishlatiladi. Yagona hisob-kitob bu to‘plamga, skalyar ko‘paytirishga tegishli. Bu guruh qonunining timsoli: $P \in E(F_q)$ nuqtasiga muvaffaqiyatli guruh operatsiyalarini qo‘llash (qo‘shish) egri chiziqdagi boshqa nuqtalar natijasida hosil bo‘ladi. Agar nuqtaga qo‘llaniladigan qo‘shimchalar soni elliptik egri guruhning tartibiga teng bo‘lsa, natija asl nuqta bo‘ladi.

$E(\mathbb{F}_q)$ egri chizig’ida skalyar ko‘paytirish P nuqtaning k qo‘shimchasini hisoblashni bildiradi va kP bilan belgilanadi. Bu jarayonda ma’lum qoidalar to‘plami orqali $Q = kP$ bo‘ladigan boshqa $Q \in E(F_q)$ nuqtani topish uchun skalyar ko’paytirish $k \in N$ va egri chiziq $P \in E(F_q)$ nuqtadan foydalaniladi. Skalyar ko‘paytirishni amalga oshirish uchun ko‘plab usullar taklif qilingan, jumladan: ikkilantirish va qo'shish, NAF, Montgomery zinapoyasi va boshqalar [1].

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2023

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-3, ISSUE-5

Bu usullarning barchasi ma’lum bir elliptik egri chiziq uchun aniqlangan guruh operatsiyalariga asoslangan bo’ladi.

EECH asosiy guruh amallari bo’lib nuqtalarni qo‘shish

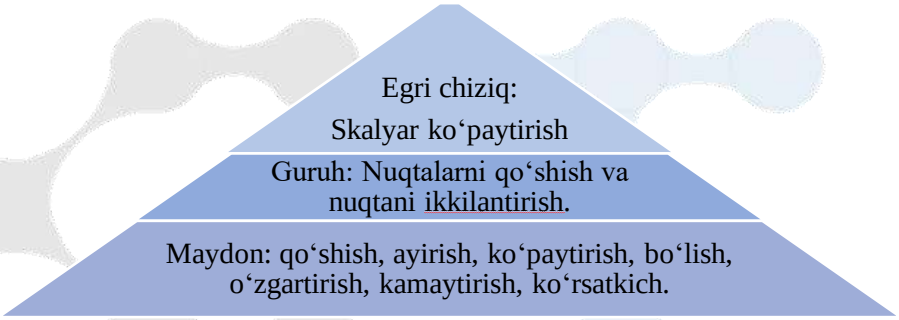
$$\boldsymbol{P} + \boldsymbol{Q} \; \forall \; \boldsymbol{P}, \boldsymbol{Q} \; \in \boldsymbol{E}(\mathbb{F}_{\boldsymbol{q}}) \qquad \textbf{(1)}$$

hamda nuqtalarni ikkilantirish

$$\boldsymbol{P} + \boldsymbol{P} \; \forall \; \boldsymbol{P} \; \in \boldsymbol{E}(\mathbb{F}_{\boldsymbol{q}}) \qquad \textbf{(2)}$$

hisoblanadi.

Quyida EECH amallarining turli darajalari ko‘rsatilgan (1.1-rasm).



1.1-rasm. EECH dagi operatsiyalarning darajalarga bo‘lingan shakli

Elliptik egri chiqizlarga asoslangan shifrlash algoritmlari

Ochiq kalitli shifrlash tizimlarida har bir A ob‘ektida ochiq kalit P_A va tegishli shaxsiy kalit a mavjud bo‘ladi. Xavfsiz tizimlarda berilgan P_A dan a ni hisoblash vazifasi qiyin. Ochiq kalit E_{P_A} shifrlovchi o‘zgartirishni belgilaydi, maxfiy kalit D_a rasshifrovkalovchi o‘zgartirishni belgilaydi. A tomonga m xabar yuborishni istagan har qanday ob‘yekt B, A tomonning P_A ochiq kalitining haqiqiy nusxasini oladi, $c = E_{P_A}(m)$ shifrlangan matnni hosil qiladi va uni A tomonga yuboradi [2]. c ni rasshifrovkalash uchun A tomon, asl xabarni olish uchun $m = D_a(c)$ rasshifrovkalash o’zgartirishni qo'llaydi.

Hozirgi kunda EECH asoslangan El-Gamal, ECIES kabi algoritmlar mavjud bo‘lib ular faktorzatsiyalash va diskret logarifmlash masalalariga qaraganda kalit o‘lchami kichik bo‘lganligi bilan faqrlanadi.

1.1-jadval

ECIES va RSA algorimtlari kalit uzunliklarini solishtirma tahlili

Xavfsizlik darajasi (bit)	RSA kalit uzunligi (bit)	ECIES kalit uzunligi (bit)
80	1024	160-223
112	2048	224-255
128	3072	256-283
192	7680	384-511
256	15360	512-571

Kalit o'lchamidagi afzallik apparatga kichikroq talablarni qo'yish imkonini beradi (masalan, bufer, operativ xotira va jismoniy xotira hajmiga; kalitlarni tarmoq orqali uzatishda kanalning o'tkazish qobiliyatiga). ECIES ning boshqa kriptografik algoritmlarga nisbatan muhim kamchiligi turli standartlar (ANSI X9.63, IEEE 1363a, ISO/IEC 18033-2 va SECG SEC 1) bilan tavsiflangan ECIES ning bir nechta versiyalarining mavjudligidir. Ushbu standartlar o'rtasidagi farqlar ECIES

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2023

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-3, ISSUE-5

komponentlarini (KA, KDF, ENC, MAC, HASH) amalga oshirish uchun maxsus funksiyalar va parametrlarni tanlashdir. Kamchilik shundaki, barcha standartlarga javob beradigan ECIES versiyasini amalga oshirish mumkin emas.

Elliptik egri chiqizlarga asoslangan elektron raqamli imzo algoritmlari

Xabarning raqamli imzosi - imzolovchining shaxsiy kalitiga va imzolanayotgan xabarga bog'liq bo'lgan koddir. Imzolar doim tekshirilishi kerak; agar biror tomon hujjatni imzolaganligi to‘g‘risida nizo yuzaga kelsa, xolis uchinchi shaxs ushbu masalani imzolovchining ochiq kalitidan foydalangan holda hal qilishi kerak bo’ladi [3].

ECDSA (Elliptic Curve Digital Signature Algorithm) - raqamli imzoni yaratish uchun ochiq kalit algoritm bo‘lib, tuzilishi bo'yicha DSA ga o‘xshash, lekin undan farqli o‘laroq, cheklangan sonli maydonda emas, balki elliptik egri chiziqdagi nuqtalar guruhida aniqlangan amallar bilan farqlanadi.

Quyidagi EECH asoslangan elektron raqamli imzo algoritmlari tahlili keltirilgan (1.2-jadval)

1.2-jadval

EC-DSA va EC-KCDSA algoritmlarning qiyosiy tahlili

Sxema	Chekli maydon	q
EC-DSA	$GF(p)$ yoki $GF(2^m)$	$q > 2^{160}$
EC-KCDSA	$GF(p), GF(2^m)$ yoki $GF(p^m)$	$\|q\| > 128 + 32i, (i = 0,1, \dots ,4)$

Sxema	Imzoni hisoblash	Imzoni tekshirish
EC-DSA	Shaxsiy imzo: $x \in_r Z_q^*$	Ochiq kalit: $y = xG$
	$k \in_r Z_q^*$ $r = \pi(kG) \ mod \ q$ $s = k^{-1}(rx + h(m)) \ mod \ q$	$u_1 = s^{-1}r \ mod \ q$ $u_2 = s^{-1}h(m) \ mod \ q$ $\pi(u_1 y + u_2 G) \ mod \ q = r?$
EC-DSA	Shaxsiy imzo: $x \in_r Z_q^*$	Ochiq kalit: $y = \bar{x}G \ (\bar{x} = x^{-1} \ mod \ q)$
	$k \in_r Z_q^*$ $r = h(kG)$ $s = x(k - r \oplus h(z\|\|m) \ mod \ q$	$e = r \oplus h(z\|\|m) \ mod \ q$ $h(sy + eG) = r?$

Elliptik egri chiqizlarga asoslangan kalitlarni tarqatish algoritmlari

Kalit o'rnatish protokolining maqsadi ochiq tarmoq orqali muloqot qiladigan ikki yoki undan ortiq ob'ektlarni umumiy maxfiy kalit bilan ta'minlashdir. Keyinchalik, maxfiylik yoki ma'lumotlar yaxlitligi kabi kriptografik maqsadlarga erishish uchun kalit simmetrik kalit protokolida ishlatilishi mumkin [4].

Elliptik egri chiziqlarga asoslangan Diffie-Hellman hamda Menezes-Qu-Vanston kalitlarni taqsimlash algoritmlari mavjud.

MQV algoritmi Diffi-Hellman algoritmiga nisbatan elliptik egri chiziqlar konteksida yaxshiroq xavfsizlikni ta’minlaydi. Biroq MQV ning aloqa qiluvchi tomonlarning ochiq kalitlarini autentifikatsiya qilish uchun sertifikatlashtirish organi (CA) kabi ishonchli uchinchi tomondan foydalanishni talab etadi. Agar sertifikatlashtirish markazi buzilgan yoki uning infratuzilmasi

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2023-5.384 ResearchBib IF: 8.848 / 2023

xavfsiz bo‘lmasa, bu qo‘shimcha murakkablik va potensial zaifliklarni keltirib chiqarilishi mumkin.

ECMQV ning umumiy sirdan olingan seans kalitni taqdim etsada, u takroriy hujumlar yoki xabarlarni buzishdan qo‘shimcha himoya qilmaydi. Shu sababli, almashilgan xabarlarning yaxlitligi va haqiqiyligini ta'minlash uchun xabarlar autentifikatsiya kodlari (MAC) kabi qo'shimcha kriptografik mexanizmlardan foydalanish muhim ahamiyatga ega.

Adabiyotlar ro‘yxati

1. Z. Liu, E. Wenger, and J. Großschädl, MoTE-ECC: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks, pp. 361–379. Cham: Springer International Publishing, 2014.

2. C. Lederer, R. Mader, M. Koschuch, J. Großschädl, A. Szekely, andS. Tillich, “Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks,” in Proceedings of the 3rd IFIP WG 11.2 International Workshop on Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks, WISTP ’09, (Berlin, Heidelberg), pp. 112–127, Springer-Verlag, 2009.

3. Akbarov Davlatali Yegitaliyevich, Xasanov Po‘lat Fattoxovich, Xasanov Xislat Po‘latovich, Axmedova Oydin Po‘latovna, Xolimtayeva Iqbol Ubaydullayevna “Kriptografiyaning matematik asoslari”. O‘quv qo‘llanma. – Toshkent. TATU. 2018 – 208 bet.

4. Z. Liu, J. Weng, Z. Hu, and H. Seo, “Efficient Elliptic Curve Cryptography for Embedded Devices,” ACM Trans. Embed. Comput. Syst., vol. 16, pp. 53:1–53:18, Dec. 2016.

5. W. Diffie and M. Hellman “New directions in cryptography” Information Theory, IEEE Transactions on, vol. 22, pp. 644 – 654. 1976.