ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO‘LLANISHI

Allanov Orif Menglimuratovich
TATU, Kiberxavfsizlik va kriminalistika kafedrasi mudiri, phd.
E-mail: orif_allanov@mail.ru

Jabborov Sherzod Nabijon o‘g‘li
TATU magistranti
E-mail: 3336360dhdh@gmail.com

ANNOTATSIYA

Ushbu maqolada Elliptik egri chiziq strukturasi va ularning ahamiyati, kriptografik tizimlarda Elliptik egri chiziqlarning qo'llanilishi tavsiflangan.

Kalit so‘zlar: diskret-logarifmlash, faktorlash, smart-kartalar, elliptik, chekli-maydon, nosimmetrik, singulyar

APPLICATION OF ELLIPTICAL CURVES IN CRYPTOGRAPHY

ABSTRACT

This article describes the structure of an elliptical curve and their significance, the application of elliptical curves in cryptographic systems.

Key words: discrete-logarithm, factoring, smart cards, elliptical, finite-field, no-symmetric, singular

EECh nazariyasini yaratishda so‘nggi qadimiy grek matematigi Diofantdan boshlab o‘tmishning ko‘pgina eng yirik olimlari qatnashgan. EECh gruppasi strukturasini mashhur fransuz matematigi Anri Puankare taklif etgan. Yillar davomida EECh hyech qanday amaliy ahamiyatga ega bo‘lmagan sof matematika sohasi bo‘lib kelgan. O‘tgan asrning 80-yillarida EECh katta sonlarni faktorlash algoritmlarini tuzish sohasida qo‘llanila boshladi [1] va bu qo‘llanishlar orqali kriptografiya sohasiga kirib keldi (nosimmetrik tizimlar, psevdotasodifiy sonlarni generasiyalash). Elliptik kriptografiyada haqiqiy burilish 1985 yilda N. Koblis va V. Miller ilmiy ishlari [2] chop etilgandan so‘ng yuz berdi. Shu damdan boshlab mashhur jahon kritologlari elliptik kriptografiya bilan shug‘ullana boshladilar.

Faktorlash va EECh gruppasida diskret logarifmlash murakkabliklarini taqqoslama tahlili EEChlarning bahslashuvdan holi afzalliklarini namoyon etdi [3].

1.1- jadvalda taqqoslama ma’lumotlar keltirilgan (ma’lumotlar tub maydonda diskret logarifmlash muammosi uchun ham oson hisoblanadi).

1.1-jadval

Kriptotahlil murakkabliklari bo‘yicha ma’lumotlar

Almashtirish moduli uzunligi	EECh gruppasida kriptotahlil murakkabligi	RSA modulini faktorlash murakkabligi
192 bit	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 bit	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 bit	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 bit	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

XXI asrning boshidan boshlab nosimmetrik kriptografiyaning an’anaga aylanib qolgan kriptotizimlardan bardoshliligi EECh gruppasida diskret logarifmlash muammosining murakkabligiga asoslangan tizimlarga o‘tish boshlangani ko‘zga tashlandi [4].

Elliptik kriptografiyaga alohida qiziqish quyidagi sabablar bilan bog‘liq:

•birinchidan, diskret logarifmlash va faktorlash muammolarini yechishga qaratilgan sonli maydon va halqalarda n moduli bo‘yicha sonlar silliqligi xossasidan foydalanadigan umumlashgan g‘alvir usuliga asoslangan tezkor algoritmlarning yuzaga kelishi. EECh gruppasida esa silliqlik tushunchasi nuqtalarga tegishli bo‘lib, tezkor kriptotahlillash algoritmlarini tuzish imkoniyatini bermaydi;

•ikkinchidan, EECh gruppasida nisbatan qisqa kalit uzunligi asosida kriptotizimlar ishlab chiqarish imkoniyati mavjudligi. Bular simsiz kommunikasiyalarda va resurs cheklangan hollarda (smart-kartalar, mobil qurilmalar) asosiy hisoblanadi. Masalan, EECh gruppasida tuzilgan kalitning binar uzunligi 150 dan 350 gacha bo‘lgan qurilmalarda an’anaviy qurilmalardagi kalitning binar uzunligi 600 dan 1400 gacha bo‘lgandagidek kriptografik bardoshlilik darajasiga erishiladi.

Yuqorida keltirilgan sabablar AQSh va Rossiya Federasiyasida amaldagi standartlarni elliptik kriptografiyaga oid standartlar bilan almashtirishga olib keldi. Hozirgi kunda EEChlarga asoslangan algoritmlar ko‘plab xalqaro, milliy va sohaga oid standartlar qatoridan o‘rin olgan. Elliptik kriptografiyada foydalanish uchun asosan $GF(2^m)$ maydonida aniqlangan singulyar yoki GF(p) maydonida aniqlangan nosupersingulyar EEChlardan foydalanish tavsiya etiladi. Barcha hollarda EECh gruppasida katta tartibga ega bo‘lgan elementlar mavjudligiga ishonch hosil qilish muhimdir.

Kriptografiyada chekli algebraik strukturalarda, masalan, chekli maydonlarda berilgan EEChdan keng foydalaniladi. Tub maydon GF(p) da berilgan EECh

$$y^2 = x^3 + ax + b \ (\text{mod } p)$$

taqqoslamaning $P = (x, y)$ nuqtalari (yechimlari) to‘plamini tashkil etadi. Bu yerda a va b kattaliklari $4a^3 + 27b^2 \neq 0 \ (\text{mod } p)$ shartini qanoatlantiruvchi doimiylar, $p > 3$. To‘plam gruppani tashkil etishi uchun unga cheksiz uzoqlashgan $O_{Ye} = (x, \infty)$ nuqta birlashtiriladi, natijada gruppa tashuvchisi $E = \{14 \text{ yechimlari}\} U\{0\}$ ko‘rinishni oladi. Mazkur gruppaning kriptografiya uchun asosiy amali nuqtalarni takroran m marta qo‘shish amali [m]P bo‘lib, uni [m] ga ko‘paytirish deb ataladi va u rekursiv suratda amalga oshiriladi. Oshkora kriptografiyada yaratilgan ko‘pchilik algoritmlarning EEChli analoglari ishlab chiqilgan. Elliptik egri chiziqli kriptotizimlar kriptobardoshliligi EEChda diskret logarifmlash muammosining murakkabligi bilan belgilanadi.

EECh nuqtalari ustida amallar bajarish masalalari yechimlari murakkabliklariga asoslangan nosimmetrik algoritmlarni yaratishda kriptotizimning har bir i - foydalanuvchisining shaxsiy kalitini ifodalovchi k_i^M – son bo‘yicha hisoblanadigan $[k_i^M]G = Q_i = (x_i{}^0, y_i{}^0)$ - ochiq kalit generasiya qilinadi, bu yerda G -tanlab olingan elliptik egri chiziqqa tegishli barchaga ma’lum bo‘lgan hosil qiluvchi (generator) nuqta. Bu yerda $G = (x_G, y_G)$ va $Q_i = (x_i{}^0, y_i{}^0)$ – nuqtalarni bilgan holda k_i^M - -shaxsiy kalitni aniqlash o‘zining rasional yechimiga ega emas.

Kriptotizimning j - -foydalanuvchisi M - ochiq ma’lumotni shifrlab, C - shifrlangan ma’lumotni i-foydalanuvchiga jo‘natishi uchun, i - foydalanuvchining barchaga ma’lum bo‘lgan ochiq kaliti $Q_i = (x_i{}^0, y_i{}^0)$ dan foydalanadi, ya’ni $E_{(x_i{}^0, y_i{}^0)}(M) = C$ shifrmatnni i-foydalanuvchiga ochiq aloqa tarmog‘i orqali yuboradi. Bu $E_{x_i^0}(M) = C$ (yoki $E_{x_i^0}(M) = C$ yoki $E_{(x_i{}^0, y_i{}^0)}(M) = C$) - shifrma’lumotni qabul qilib olgan i –foydalanuvchi, faqat uning o‘ziga ma’lum bo‘lgan o‘zining shaxsiy kaliti k_i^M bilan deshifrlaydi, ya’ni $D_{k_i^M}(C) = M$ – ochiq ma’lumotga ega bo‘ladi. Shifrlash qoidasini aniqlovchi akslantirish $E_{(x_i{}^0, y_i{}^0)}(M) = C$ bir tomonlamalik xususiyatiga ega bo‘lishi kerak, ya’ni E - akslantirish, $Q_i = (x_i{}^0, y_i{}^0)$ ochiq kalit va C - shifrmatnni bilgan holda M - ochiq ma’lumotni aniqlash imkoniyati yo‘q bo‘lishi kerak.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. 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.
2. 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.
3. 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.
4. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition. Chapman & Hall/CRC, 2nd ed., 2012.