KOMPYUTER TARMOG‘IDA ELLIPTIK GURUHLARDAGI KORXONALARNING MAXFIY KALITLARNI TARQATISH XIZMATI

O‘tkirbek Xamrakulov Sharobiddin o‘g‘li
Assistent. Toshkent davlat texnika universiteti
xamrakulovutkirbek@gmail.com

Annotatsiya: *Ushbu maqolada Tartibi tub son bo‘lgan elliptik guruhlarni hisoblash uchun Perl dasturi ishlab chiqilgan va guruhning istalgan nuqtasi bir xil tartibdagi tsiklik kichik guruh uchun generator hisoblanadi. Dasturiy ta’minot FreeBSD operatsion tizimida Perl tilida yozilgan va korporativ kompyuter tarmog‘ining tugunlari o‘rtasida ma’lumotlar uzatishni himoya qilish uchun bir martalik seansning maxfiy kalitlarini ta’minlash uchun ishlatiladi.*

Kalit so‘zlar: *elliptik kriptografiya, maxfiy kalit yetkazib berish, Perl.*

Kirish

Korxonada kompyuter tarmog‘ining axborot xavfsizligini ta’minlashning umumiy usuli - bu ulanish orqali ikki tomonlama ma’lumotlar almashinuvini yoki katta ma’lumotlar paketini bir martalik uzatishni amalga oshiradigan yagona maxfiy kalit bilan barcha uzatiladigan ma’lumotlarni doimiy shifrlashdir. Maqsad tarmoq kommutatorida yoki yo‘naltirish marshruti bo‘ylab tugunlardan birida ma’lumotlarni olish uchun xakerlik dasturini o‘rnatgan tajovuzkor etarli miqdorda to‘plangan bir xil kalit bilan shifrlangan ma’lumotlar miqdorining kriptotahlilini amalga oshirish.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Tarmoqni tashkil qilishda bitta ulanish yoki bitta udp-paket uchun bir martalik maxfiy kalitlardan foydalanish uchun uzluksiz shifrlash taklif etildi. Bundan tashqari, ularning kalit uzunligi 12-16 ta raqamlarda yetarli kriptografik quvvatni ta’minlaydi. Bir juft tarmoq abonentlari uchun bir martalik kalitni yetkazib berish algoritmi raqamli

Abel guruhida emas, balki elliptik egri chiziqning Abeliya nuqtalari guruhida amalga oshiriladi, guruhning nisbatan kichik tartibi esa bir xil kriptografik kuchni ta’minlaydi. ko‘p sonli mintaqada raqamli guruh bilan va hisob-kitoblarning hajmi va vaqti sezilarli darajada kamroq. Xuddi shu kriptografik quvvat juda kichikroq buyurtma bilan ta’minlanadi.

Mualliflar Weyershtrassa shaklidagi elliptik egri chizig‘i uchun juda kichik [1] tartibli (1000 tagacha) guruhlar misollaridan foydalangan holda elliptik guruhlarni tasvirlash uchun modelni nashr etdilar, bu elliptik egri chiziqlarning etarlicha keng sinfi izomorf o‘zgarishlar bilan kamayadi:

$$Y^2 = X^3 + A \cdot X + B(\mathrm{mod}\, P).(1)$$

Quyidagi formula maxfiy kalitlarni tarqatish xizmatining elliptik guruhlarini olish uchun xizmat qiladi. P asosiy modulining qiymati elliptik guruh elementlarining (elliptik egri nuqtalari) X: Y koordinatalarining maksimal qiymatini cheklaydi, guruh faqat butun sonning koordinatali nuqtalar orqali hosil bo‘ladi. Har bir element elliptik egri chiziq nuqtalari sinflaridan biriga kiradi, har bir sinfda nuqtalar soni cheksiz va koordinatalarning qiymati koordinata o‘qlarining ijobiy va salbiy yo‘nalishlarida cheksizdir. Biroq, sinflar soni chekli, har bir sinf koordinata o‘qlarining birinchi kvadrantida o‘zining yagona soni bilan ifodalanadi (X > 0, Y > 0).

Kriptografik algoritm tartiblangan Abel guruhiga asoslangan, ya’ni. Guruhning har qanday elementlari uchun qaysi biri oldingi va qaysi biri keyingi ekanligi ma’lum va birinchi va oxirgi element mavjud. Raqamli guruhlar uchun bu aniq hisoblanadi, elliptik guruhda esa, uning barcha nuqtalarini hisoblagandan so‘ng, bu tartib aniqlanadi. Biz davriy elliptik kichik guruhni elliptik guruh nuqtalarining tartiblangan kichik to‘plami deb ataymiz, unda birinchi element GT hosil qiluvchi nuqta deb ataladi, har bir keyingisi joriy T nuqtasini GT ga qo‘shish natijasida olinadi, oxirgi element esa noto‘g‘ri element θ, u (nol elementning xususiyati bo‘yicha) yana GT bilan birga keladi va davriy kichik guruhning barcha bir xil nuqtalarini bir xil ketma-ketlikda takrorlaydi. Agar davriy elliptik kichik guruh elliptik guruhning barcha nuqtalarini o‘z

ichiga olmasa, u holda Lagranj teoremasi [2, c.19] bo‘yicha kichik guruhning tartibi va ko‘rsatkichi guruh tartibining bo‘luvchilari hisoblanadi. Kichik guruh indeksi elliptik guruh tartibini kichik guruh tartibiga bo‘lish natijasida hosil bo‘lgan butun sondir.

Katta raqamlar oralig‘ida 2,3,5,6 indeksli kichik guruhlarda kripto-algoritmni amalga oshirish mumkin, ammo elliptik nuqtalarning faqat yarmi qo‘llaniladi, guruh uchinchi, 1/5 yoki 1/6 va elliptik kichik guruh tartibining talab qilinadigan minimal qiymatini ta’minlash uchun kattaroq uzunlik oralig‘ida asosiy modul P ni topish kerak. Ammo biz, iloji bo‘lsa, unumdorlikni oshirish uchun kichik uzunlikdagi raqamlar oralig‘idan foydalanmoqchi bo‘lsak, unda biz 1 indeksli kichik guruhlardan foydalanishimiz kerak, ularning tartibi OrdEG guruhining tartibiga va barcha nuqtalarga teng bo‘lgan elliptik guruhdan foydalaniladi. Bunday kichik guruhning hosil qilish nuqtasi generatsiya nuqtasi deb ataladi. Agar elliptik guruhning tartibi bo‘linuvchisi bo‘lmagan tub son bo‘lsa, u holda Lagranj teoremasiga ko‘ra, bunday elliptik guruhning istalgan nuqtasi GT hosil qiladi va hosil qilgan har qanday kichik guruhlarning tartib qiymati teng bo‘ladi. guruh tartibi esa har qanday kichik guruxning barcha nuqtalarini o‘z ichiga oladi, lekin ularning har biri o‘ziga xos nuqta almashtirishga ega bo‘ladi. Ushbu ishda faqat shunday ko‘rinishdagi holatlar ko‘rib chiqiladi. OrdEG guruhining tartibi oddiy P modulining modulidan kichik, teng yoki undan katta bo‘lishi mumkin, ammo Hasse teoremasiga [2, p.105] ko‘ra bu qiymatlar orasidagi farqning mutlaq qiymati elliptik guruhni tashkil etuvchi oddiy modulning kvadrat ildizidan ikki baravar ko‘p bo‘lmagan:

$$|OrdG - P - 1| < 2 \cdot \sqrt{P} \quad (2)$$

Elliptik guruhlarni hisoblash va bir juft korporativ tarmoq abonentlariga maxfiy kalitni etkazib berish uchun dasturiy ta’minot, shu jumladan Perl moduli ishlab chiqilgan EGopResearch.pm, shu jumladan funksiyalar:

- EG mod P(1) tenglamasining o‘ng tomonidagi X ko‘phadni hisoblash;
- ikkita mos kelmaydigan EG elementini qo‘shish;
- EG elementining o‘ziga qo‘shilishi (ikki barobar);

•EG elementining o‘zi bilan bir necha marta qo‘shilishi (qo‘shimchalar soniga ko‘paytirish);

•EG elliptik guruhining θ dan tashqari barcha elementlarini hisoblash;

•bir nechta yordamchi funktsiyalar.

NATIJA

1-rasmda guruhni tashkil etuvchi oddiy modullar diapazonida X (a=2, b=-4) ko‘phad uchun elliptik guruhlarni hisoblash natijasi ko‘rsatilgan. Ushbu diapazonning qamrovi 10000 butun son, Ulardan 721 tasi tub sonlardir.

P=990761 a=2 b=-4; ordEG=991717; 956; 1990.74;

P=990851 a=2 b=-4; ordEG=992707; 1856; 1990,83;

P=991693 a=2 b=-4; ordEG=991873; 180; 1991,68;

P=991703 a=2 b=-4; ordEG=990397;-1306; 1991,69;

P=991741 a=2 b=-4; ordEG=993557; 1816; 1991,72;

P=992269 a=2 b=-4; ordEG=991429; -840; 1992,25;

P=992429 a=2 b=-4; ordEG=993557; 1128; 1992,41;

P=992591 a=2 b=-4; ordEG=993319; 728; 1992,58;

P=992809 a=2 b=-4; ordEG=992417; -392; 1992,80;

P=993683 a=2 b=-4; ordEG=995119; 1436; 1993,67;

P=993703 a=2 b=-4; ordEG=993943; 240; 1993,69;

P=994237 a=2 b=-4; ordEG=994723; 486; 1994,23;

P=995471 a=2 b=-4; ordEG=995117; -354; 1995,47;

P=995941 a=2 b=-4; ordEG=995987; 46; 1995,94;

1-rasm. P=990000-999999 oralig‘ida OrdEG bosh tartiblarining elliptik guruhlari

Argumentlar qo‘shimchalarning maxfiy soni, hosil qiluvchi nuqta, oddiy P moduli, (1) tenglamadagi X ko‘phadning koeffitsientlari. Hisoblangan Y1_2 elementi

1-boshlovchi tomonidan 2-maqsadga amalga oshirilgan umumiy qiymatdir (EG elementi), bu va ishlab chiqaruvchi nuqta maqsad xostga yuboriladi, ular sir emas, lekin u to‘liq uchdan uchiga shifrlanganligi sababli, paketli ma’lumotlar avvalgi ma’lumotlar almashinuvi uchun ishlatilgan maxfiy kalit bilan shifrlangan. Bu avvalgi bir martalik kalitni ikkinchi marta ishlatishning kamdan-kam holi bo‘lib, keyin darhol yo‘q qilinmaydi foydalanish, lekin keyingi foydalanishdan oldin yangi qiymat bilan maxfiy kalit jadvalida bekor qilinadi. Har birida maxfiy kalitlar jadvali mavjud xost protokolda bo‘lgani kabi [3], lekin bu yerda u bir martalik kalitlarni o‘z ichiga oladi.

Belgilangan xost paketni qabul qilib, o‘zining maxfiy tasodifiy qiymatini yaratadi, u n1 = 482507 bo‘lsin, uning umumiy qiymati Y2_1 boshlang‘ich xostiga yuboriladi va yangi bir martalik maxfiy kalit K2_1 nusxasini hisoblaydi:

./mk_nTxy.pl 482507 343122:460585 993683 2 -4 # natija Y2_1 = 264641:18878

./mk_nTxy.pl 482507 229779:952572 993683 2 -4 # natija K2_1 = 980362:744294

2-maqsadli xost Y2_1-ni kalit jadvalidagi eski bir martalik kalit bilan shifrlangan 1-hostga yuboradi va keyin bu eski bir martalik kalit qiymatini yangi hisoblangan K2_1 qiymati bilan qoplaydi. Boshlovchi xost Y2_1 qiymatini olgan holda, 2-host bilan bir martalik kalit nusxasini hisoblab chiqadi:

./mk_nTxy.pl 765312 264641:18878 993683 2 -4 # natija K1_2 = 980362:744294

XULOSA

Xulosa qilib 2-xostda bo‘lgani kabi, 1-hostda n1 (n2, GT) va 2-hostda n2 (n1 GT) bo‘ladi - bu xostlardagi GT qo‘shimchalari soni $n1 \cdot n2$ ko‘paytmasiga teng. Yangi bir martalik kalit K1_2 2-xostning shaxsiy kalit jadvalidagi oldingi qiymatni almashtiradi. Ikki nuqta maxfiy kalitdan olib tashlanadi va X, Y koordinatalari maxfiy kalit sifatida 12 bitli o‘nlik sonni hosil qilish uchun birlashtiriladi va Serverdagi EG faylining hajmi taxminan 7 Mb ni tashkil qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Монахов В.И., Кузьмич И.В., Степанова О.П., Стрельников Б.А. Использование средств эллиптической криптографии для защиты информации в компьютерных сетях предприятий текстильной и легкой промышленности // Дизайн и технологии. 2014. № 44 (86). С. 124-128.

2. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. - М., КомКнига, 2012. 356 с.

3. Монахов В.И., Кузьмич И.В., Степанова О.П., Стрельников Б.А. Протокол защищенных соединений для сети предприятия // Альманах мировой науки. 2017. №1-1(16). С. 58- 62.