Liet. matem. rink, **46***, spec. nr.*, 2006, 112–115

Matricinė diskretinio logaritmo problema*

Povilas TVARIJONAS, Gediminas Simonas DOSINAS,
Eligijus SAKALAUSKAS (KTU)
el. paštas: povilas.tvarijonas@ktu.lt, gediminas.dosinas@ktu.lt, esakal@asi.lt

1. Įvadas

Diskretinio logaritmo problema (DLP) plačiai naudojama viešojo rakto kriptografinėse sistemose [2]. Jos pagrindu sukurtas Diffie–Hellman'o raktų apsiketimo protokolas, El-Gamalio kriptosistema, skaitmeninio parašo sistema, kuri realizuota standartizuotame algoritme DSA (Digital signature algorithm), ir t.t.

Kartu su kriptografinių algoritmų kūrimu, kurių saugumo garantas yra DLP algoritminio sprendimo sudėtingumas, vystosi ir šių algoritmų kriptoanalizės metodai. Jeigu prieš 10–15 metų užteko naudoti 2^{1024} eilės moduliarines eksponentes, kurių diskretinis logaritmavimas buvo efektyviai neįveikiama algoritminė problema, tai šiuo metu jau naudojamos 2^{4096} eilės moduliarines eksponentės, norint užtikrinti pakankamą saugumą prieš išvystytas tradicines kriptografines atakas. Šis skaičių dydumo išaugimas įneša tam tikrų nepatogumų kriptografinių algoritmų realizacijai, pvz. intelektualiose kortelėse.

Tačiau paskutiniuoju metu buvo atrasti kvantinės informacijos teorijos algoritmai, kurie leidžia surasti diskretinį algoritmą per polinominį laiką, skaičiaus eilės atžvilgiu [3]. Šie algoritmai gali būti realizuojami kvantiniuose kompiuteriuose, apie kuriuos šiuo metu palčiai kalbama. Prognozuojama, kad tokie kompiuteriai gali pasirodyti rinkoje artimiausių 10–15 metų perspektyvoje. Todėl visame pasaulyje plačiai vykdomi tyrimai, siekiant pakeisti tradicines kriptografines technologijas naujomis, kurioms bent jau kol kas neegzistuoja efektyvūs kriptoanalizės algoritmai.

Šiame darbe nagrinėjama matricinė diskretinio logaritmo problema (MDLP), kuri savo kokybe iš esmes skiriasi nuo įprastos DLP. Skirtumas glūdi tame, kad skaičiuojant moduliarinę eksponentę, atliekami tiktai daugybos veiksmai, tuo tarpu keliant laipsniu matricas, atliekami tiek daugybos, tiek sumos veiksmai. Tai turėtų algoritmiškai apsunkinti MDLP sprendimą ir tuo būdu padidinti MDLP pagrindu sukurtų sukurtų kriptografinių algoritmų saugumą.

2. Diskretinio logaritmo problema (DLP)

Turime baigtinę p-tosios eilės ciklinę grupę $G =< \alpha >$, kurios generatorius α, tegul $\beta \in G$, čia p – pirminis. Elemento β diskretiniu logaritmu pagrindu $\alpha \log_\alpha \beta$ vadina-

*Darbas remiamas Lietuvos respublikos valstybinio mokslų ir studijų fondo

mas skaičius

$$x \in \{0, 1, ..., p-1\}, \quad x\colon \beta = \alpha^x, \quad (x = \log_\alpha \beta). \tag{1}$$

(Lyginių teorijoje vartojamas indekso terminas $ind_q a = k : q^k \equiv a(\mathrm{mod} m)$, $k \in N$, q ir m tarpusavyje pirminiai natūralieji skaičiai [1]).

Problemą galima spręsti perrinkimo metodu, tuomet atliekamų žingsnių skaičius ekvivalentus $O(p)$, tačiau kai

$$p = 227088231986781039743145181950291021585250524967592855964532691897983114274751597764112766422771139650833937,$$

šimtas septynių ženklų skaičius, arba, pavyzdžiui, $p = 2^{6972593} - 1$, atliekamų operacijų skaičius yra didelis net ir šiuolaikiniams kompiuteriams. Diskretinio logaritmo problemos sprendimo metodų apžvalgą galime rasti [2]. Sprendžiant DLP mažo žingsnio didelio žingsnio (baby-step giant-step) arba Polardo (Pollard's rho) algoritmais vidutiniškai reikėtų atlikti $\sqrt{n}$ žingsnių. Jeigu $n \approx 2^{160}$, tai reikštų, kad reikėtų atlikti maždaug 10^{24} grupinių operacijų, o tai pareikalautų apie 10^{26} kompiuterinių komandų, tam reikėtų maždaug 10^{12} MY norint šiuos algoritmus realizuoti [4]. (MY$= 10^6 \cdot 3,15 \cdot 10^7 == 3,15 \cdot 10^{13}$ – kompiuterio, atliekančio 10^6 komandų per sekundę, atliekamų komandų skaičius per metus. Vidutinio kompiuterio greitis – 100MY. Pačio greičiausio kompiuterio 2004, IBM's BlueGene/L, greitis buvo maždaug $7,072 \cdot 10^7$MY).

3. Matricinė diskretinio logaritmo problema (MDLP)

Tarkime, kad F_p – baigtinis laukas, $|F_p| = p$, $M_n(F_p)$ – kvadratinių n-tosios eilės matricų, apibrėžtų lanke F_p, aibė, kurioje algebrinės operacijos apibrėžtos tradiciškai. Tarkime, kad $A \in M_n(F_p)$. Apibrėžiame $S(A) = \{A^k, k \in \{0, 1, 2, ..., p^{n^2}\}\}$.

Suformuluosime matricinę diskretinio logaritmo problemą. Turime $B \in S(A)$, reikia rasti mažiausią natūralųjį x, tokį, kad

$$B = A^x, \quad \text{t.y. } x = \log_A B. \tag{2}$$

4. MDLP sprendimo metodai

I. Kai p nedidelis, MDLP, kaip ir DLP, galima spręsti perrinkimo metodu. Tokiu atveju maksimalus žingsnių skaičius $N \leqslant p^{n^2}$ ir kiekviename žingsnyje gali tekti atlikti $n^3(n-1)$ algebrinių lauko operacijų, t.y. viso $N \cdot n^3(n-1)$ operacijų. Matyti, kad, kai p ir n dideli, šis algoritmas neefektyvus.

II. Pastebėsime, kad, jeigu λ – charakteringojo daugianario

$$P_A(\lambda) = \det(A - \lambda E) \tag{3}$$

šaknis, tai λ^k – charakteringojo daugianario

$$P_{A^k}(\mu) = \det(A^k - \mu E) \tag{4}$$

šaknis, nes, remiantis daugianario skaidymu dauginamaisiais, gauname

$$\begin{aligned}\det(A^k - \lambda^k E) &= \det\left(A^k - (\lambda E)^k\right)\\ &= \det\left((A-\lambda E)(A^{k-1} + A^{k-2}\cdot\lambda + A^{k-3}\cdot\lambda^2 + .. + A\cdot\lambda^{k-2} + \lambda^{k-1}\cdot E)\right)\\ &= \det(A-\lambda E)\cdot\det(A^{k-1} + A^{k-2}\cdot\lambda + ... + \lambda^{k-1}E) = 0.\end{aligned}$$

Todėl, norėdami išspręsti (2), randame charakteringojo daugianario $P_A(\lambda)$ šaknį λ_1, lauke F_p, arba, jeigu daugianaris $P_A(\lambda)$ yra pirminis (neskaidus) žiede $F_p[x]$, šio lauko paprastajame algebriniame plėtinyje [1], [5]. Kartais iš anksto galima nustatyti daugianario šaknų skaičių lauke F_p, pavyzdžiui, remiantis König–Rados teorema [5]. Kai kurie šaknų ieškojimo algoritmai lauke F_p arba jo algebriniame plėtinyje siūlomi [5], nors dalies jų charakteris daugiau tikimybinis. Suradę charakteringojo daugianario $P_A(\lambda)$ šaknį λ_1 nustatome kokiam mažiausiam natūraliajam k_1

$$P_B(\lambda_1^{k_1}) = 0 \tag{5}$$

bei randame elemento $\lambda_1 \in F_p$ eilę m_1, t.y. mažiausią natūralųjį m_1, tokį, kad $\lambda_1^{m_1} = e$ [5]. Tuomet (2) lygties sprendinys turės pavidalą $x = k\cdot m_1 + k_1$.

Nuo dabar galima taikyti metodus, skirtus įprastai DLP spręsti, pvz. „mažo žingsnio didelio žingsnio“ metodą.

Apskaičiavus A^{k_1} bei A^{m_1} lieka didelio žingsnio pagalba ieškoti mažiausio natūraliojo k, tokio, kad

$$A^{k\cdot m_1 + k_1} = B. \tag{6}$$

III. Norėdami padidinti žingsnį randame keletą skirtingos eilės charakteringojo daugianario $P_A(\lambda)$ šaknų $\lambda_1, \lambda_2, ..., \lambda_s$. Jeigu jų eilės atitinkamai $m_1, m_2, ..., m_s$ tarpusavyje pirminės, kiekvienai šakniai λ_i nustatome mažiausią k_i, tokį, kad

$$P_B(\lambda_i^{k_i}) = 0, \quad i = 1, 2, ..., s. \tag{7}$$

Pasinaudojame kiniečių teorema apie liekanas [6], kuri tvirtina:

Jeigu $m_1, m_2, ..., m_s$ tarpusavyje pirminiai skaičiai, tai pirmojo laipsnio lyginių sistema

$$\begin{aligned} x &\equiv k_1 (\mathrm{mod} m_1),\\ x &\equiv k_2 (\mathrm{mod} m_2),\\ &\cdots\cdots\cdots\\ x &\equiv k_s (\mathrm{mod} m_s) \end{aligned} \tag{8}$$

turi sprendinius, sutampančius moduliu $m = m_1\cdot m_2\cdot ...\cdot m_s$.

Pasinaudojus Gauso algoritmu [2], [7] lygčių sistemos (8) sprendinys, o tuo pačiu ir (2) lygties sprendinys

$$x = k_0 (\mathrm{mod} m), \tag{9}$$

čia

$$k_0 = \sum_{i=1}^{s} k_i M_i N_i,$$

$$M_i\colon\ m_1 \cdot m_2 \cdot \ldots \cdot m_s = M_i \cdot m_i,$$

$$N_i\colon\ M_i \cdot N_i \equiv 1 (\mathrm{mod} m_i), \quad i = 1, 2, \ldots, s.$$

(Gauso algoritmo realizavimui reikia $\mathrm{O}((\lg m)^2)$ laiko sąnaudų [2].)

Taigi tuomet (2) lygties sprendinio radimo procedūra pasinaudojus lygybe

$$A^{k \cdot m + k_0} = B,$$

bus atliekama su didesniu žingsniu m.

5. Išvados

1. Iš pateiktos analizės matome, kad MDLP sprendimas gali būti suvestas į daugianario virš baigtinio lauko šaknų suradimo algoritmą ir į standartinę DLP, tačiau su mažesne paieškos aibe.
2. Šiuo metu nežinomi deterministiniai polinominiai algoritmai, leidžiantys surasti daugianario virš baigtinio lauko šaknis.
3. Jeigu daugianario virš baigtinio lauko šaknų suradimo algoritmas bus sudėtingesnis už standartinę DLP, tai MDLP tampa sudėtingesne algoritmine problema tuo pačiu užtikrinančia didesnį jos pagrindu sukurtų algoritmų kriptografinį saugumą.

Literatūra

1. K. Bulota, P. Survila, *Algebra ir skaičių teorija*, t. 2, Mokslas, Vilnius (1990).
2. A. Menezes, P.C. Van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1996).
3. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, **26**, 1484–1509 (1997).
4. A. Odlyzko, Discrete logarithms: the past and the future, in: *Designs, Codes and Cryptography*, **19**(2–3), Springer (2000), pp. 129–145.
5. Р. Лидл, Г. Ниддеррейтер, *Конечные поля*, т. 1, Мир, Москва (1988).
6. К. Айерлэнд, М. Роузен, *Классическое введение в современную теорию чисел*, Мир, Москва (1987).
7. И.М. Виноградов, *Основы теории чисел*, Наука, Москва (1981).

SUMMARY

P. Tvarijonas, G.S. Dosinas, E. Sakalauskas. Discrete logarithm problem in matrix

In this paper the discrete logarithm problem in matrix in finite fields is formulated, possible ways of solution are given.

Keywords: discrete logarithms, matrix, finite fields.