PARALLEL HISOBLASHNI SHIFRLASHGA TADBIQ QILISH YO‘LLARI

Abdullayev Nodir Atamuratovich
Osiyo xalqaro universiteti magistranti.
Matrasulova Nafosat Matrasulovna
Osiyo xalqaro universiteti magistranti.
Mavlanov Aziz Bagbekovich
Khiva Ogahiy ijod maktabi o‘qituvchisi.

Annotatsiya

Ushbu maqolada shifrlash algoritmi sifatida o‘rganilgan matritsani vektorga ko‘paytirish jarayoniga parallel hisoblashni joriy qilish eksperimenti keltirib o‘tilgan.

Kalit so‘zlar

Kriptografiya, shifrlash, parallel algoritm, matritsa, vektor

KIRISH

Katta hajmdagi axborotni shifrlash muammosi nisbatan yaqinda yuqori sig‘imli o‘tkazuvchanlik qobiliyatiga ega bo‘lgan tarmoqlar paydo bo‘lishi bilan vujudga keldi.

Dastlab kriptografiya faqat matn yoki belgili ma'lumotlarni himoya qilish bilan shug‘ullangan. Biroq, zamonaviy axborot texnologiyalari va tizimlarida sezilarli darajada katta hajmdagi ma'lumotlarni uzatishni talab qiladigan texnologiyalar qo‘llanila boshlandi.

Bunday hajmdagi ma'lumotlarni shifrlash uchun juda ko‘p vaqt talab qilinadi va bunday shifrlash algoritmining samaradorligi yuqori baxolanmasligi mumkin.

Hozirgi vaqtda bu muammo ma'lumotni oqimli uzatish yoki blokli uzatish orqali hal qilinadi, bu kechikishni kamaytiradi, lekin shifrlash jarayonini tezlashtirmaydi[1]. Keyingi yechimi sifatida ko‘p protsessorli tizimlarni keltirish mumkin. Bunday holda, shifrlash bir protsessor tomonidan emas, balki parallel protsessorlar tomonidan amalga oshiriladi. Bunday tizimdan foydalanish uchun parallel shifrlash algoritmlarini ishlab chiqish kerak.

Shunday qilib, parallel kriptografiya algoritmlaridan foydalanish shifrlash uchun ketadigan vaqt miqdorini sezilarli darajada kamaytirishi mumkin.

TAHLIL VA METODOLOGIYA

Agar A_{mxn} matritsa G (N) cheklangan maydonda berilsin, agar $m \geq n$, A_{mxn} matritsa uchun bunday B_{nxm} matritsa mavjud bo‘lsa, uning ko‘paytmasi G(N) cheklangan maydondagi E_{nxn} birlik matritsaga teng bo'ladi [2], ya’ni:

$$B_{nxm}A_{mxn}(\text{mod } N) = E_{nxn}(\text{mod } N) \quad (1)$$

Ma'lumotni shifrlashda ushbu (1) tuzilmadan foydalanish mumkin. Agar biz A_{mxn} matritsani ochiq kalit sifatida, B_{nxm} matritsani esa maxfiy kalit sifatida qabul qilsak, shifrlash va deshifrlash jarayoni quyidagi qoidalarga muvofiq amalga oshirilishi mumkin[2]:

Shifrlash: $Y_{mx1} = A_{mxn} * X_{nx1} (\text{mod } N)$ (2)

Deshifrlash: $X_{nx1} = B_{nxm} * Y_{mx1} (\text{mod } N)$ (3)

Bu yerda X_{nx1} - ochiq matn blokining vektorli ko'rinishi, Y_{mx1} - shifrli matn blokining vektorli ko'rinishi.

MUHOKAMA

Yuqoridagi biz yangi shifrlash algoritmi sifatida o'rganishni davom ettirayotgan algoritmda matritsani vektorga ko'paytirishga bir nechta bor duch kelinadi.

Ushbu bosqichda biz matritsani vektorga ko'paytirishning parallel algoritmlarini ishlab chiqishni ko'rib chiqamiz[3].

A_{mxn} matritsani va n ta elementdan iborat X_{nx1} vektorni ko'paytirish amalini ko'rib chiqaylik. Ko'paytirish natijasida m o'lchamdagi Y_{mx1} vektor olinadi, uning har bir i-elementi A_{mxn} matritsaning i-qatori (bu qatorni a_i deb belgilaymiz) va X_{nx1} vektorini skalyar ko'paytirish natijasidir.

$$y_i = (a_i, X) = \sum_{j=1}^{n} a_{ij} x_j, \quad 1 \le i \le m. \qquad (4)$$

Quyida ushbu (4) ifodaning ketma-ket hamda parallel algoritmlarini tuzib hisoblash eksperimentini keltiramiz.

NATIJALAR

Ketma-ket algoritm

Dastlabki ma'lumotlar: A_{mxn} - m x n matritsa, n ta elementdan iborat X_{nx1} - vektor. Natija: Y_{mx1} - m elementli vektor. Matritsa vektorni ketma-ket ko'paytirish algoritmi quyidagicha ifodalanishi mumkin:

$y_i = y_{i-1} + a_{ij} \cdot x_j$ bu yerda $1 \le i \le m, \le j \le n$ (5)

Parallel algoritm

Matritsalarni hisoblashning ko'plab usullarida matritsalarning turli elementlari uchun bir xil hisoblash amallarini takrorlanishi odatiy holdir. Bu matritsalar hisob-kitoblarini amalga oshirishda ma'lumotlar parallelligi mavjudligini ko'rsatadi va natijada matritsa amallarining parallellashuvi ko'p hollarda ishlatiladigan kompyuter tizimining protsessorlari o'rtasida qayta ishlanayotgan matritsalarning bo'linishigacha

kamayadi. Matritsani blokga ajratish usulini tanlash ma'lum bir parallel hisoblash usulini aniqlashga olib keladi.

Matritsani vektorga ko'paytirish algoritmini ko'rib chiqamiz. Agar A matritsa kvadrat (m=n) bo'lsa, matritsani vektorga ko'paytirishning ketma-ket algoritmi $T_1 = n^2$ murakkablikka ega. Parallel hisoblashda har bir protsessor A matritsasining faqat bir qismini (qatorini) X vektoriga ko'paytiradi, bu qisimlar o'lchami n/p qatorlarga teng. Matritsa va vektorning bir qatorining skalyar ko'paytmasini hisoblashda n ta ko'paytirish amali va (n-1) ta qo'shish amalini bajarish kerak bo'ladi. Shuning uchun parallel algoritmning hisoblash hajmi quyidagi ifoda bilan aniqlanadi[3]:

$$T_p = \frac{n^2}{p} \qquad (6)$$

Bu yerda, T_p - dasturni p ta protsessorli tizimda hisoblashni bajarish vaqti,

n - matritsa o'lchami, p - parallel protsessorlar soni.

Ushbu (6) formulani hisobga olgan holda, parallel algoritmning tezligi va samaradorligi ko'rsatkichlari mos ravishda quyidagi ko'rinishga ega:

$$S_p = \frac{n^2}{n^2/p} = p \qquad (7)$$

$$E_p = \frac{n^2}{p \cdot (n^2/p)} = 1 \qquad (8)$$

Amalga oshirilgan ko'paytirish va qo'shish amallari bir xil davomiylikka ega degan farazdan foydalanamiz. Bundan tashqari, biz hisoblash tizimining bir hil ekanligini ham taxmin qilamiz ya'ni, ushbu tizimni tashkil etuvchi barcha protsessorlar bir xil ishlashga ega. Kiritilgan taxminlarni hisobga olgan holda, hisob-kitoblarga bevosita bog'liq bo'lgan parallel algoritmni bajarish vaqti:

$$T_p(calc) = [n/p] \cdot (2n-1) \cdot \tau \qquad (9)$$

Bu yerda [ ] – butun songa yaxlitlash,

τ - ko'paytirish va qo'shish amallari bir xil davomiyligi vaqti.

1-jadval.

Hisoblash eksperimenti natijalari*(qiymatlar millisekundlarda keltirilgan)*

Matritsa o'lchami	Ketma-ket algoritm	Parallel algoritm	
		1 protsessor	4 protsessor
10	0.0057	0.0319	0.0908
20	0.0137	0.0369	0.0227
30	0.0268	0.0478	0.0288
40	0.0452	0.062	0.0387
50	0.0685	0.081	0.0529
60	0.0984	0.1051	0.0723

70	0.1351	0.1377	0.095
80	0.1715	0.1762	0.1234
90	0.2186	0.2181	0.1568
100	0.2847	0.2927	0.1869

1-jadval ma'lumotlari asosida parallel algoritm va ketma-ket algoritmlardan foydalanilgandagi farqni kuzatish mumkin. Osongina ko'rish mumkinki matritsalar o'lchami kattalashgan sari bu ikki algoritm ishlagandagi farq ham sezilarli ortib boryapdi. Shunday qilib, juda katta sondagi o'lchamlar uchun parallel algoritmni ishlab chiqishda ushbu tahlil juda foydali bo'lib, bu algoritmning samaradorligini bashorat qilish, uning kuchli va zaif tomonlarini aniqlash imkonini beradi, bu esa samaradorlikni oshirish yo'llarini tanlashda ishlatilishi mumkin.

XULOSA

Ushbu algoritm katta hajmdagi ma'lumotlarni kriptografik qayta ishlash samaradorligini oshirish uchun parallel ishlov berishdan foydalanadi. Katta hajmdagi ma'lumotlar uchun shifrlash talab qilinadigan muhitda ikki yoki undan ortiq kompyuter protsessorlari o'rtasida shunga o'xshash qayta ishlash faoliyatini bo'lish uchun shifrlashni qayta ishlash oqimini o'zgartirish foydali bo'lishi mumkin. Misol uchun, agar bir nechta ma'lumotlar bloklari bir xil kriptografik operatsiya uchun rejalashtirilgan bo'lsa, bir protsessor tomonidan ketma-ket ishlov berish o'rniga, ular parallel ravishda kriptografik operatsiyani bajaradigan ikki yoki undan ortiq CPU tomonidan qayta ishlanadi. Ushbu turdagi operatsiya istalgan o'tkazish tezligiga erishish uchun kerak bo'lganda ko'plab parallel protsessorlargacha kengaytirilishi mumkin.

ADABIYOTLAR RO'YXATI:

1. *Баричев С.* "Криптография без секретов". М.: Горячая Линия - Телеком, 2004.

2. *Alisher Mavlonov.* "Investigation of the possibility of using matrix multiplication in asymmetric cryptographic systems". THE JOURNAL OF ACADEMIC RESEARCH IN EDUCATIONAL SCIENCES. VOLUME 2, ISSUE 10, 2021.

3. *А. В. Старченко, В. Н. Берцун.* "Методы параллельных вычислений". Издательство Томского университета 2013.

4. F. A.Alisherov , S.Q.Iskandarov , S.I.Khamraeva and B.B.Nurmetova (2021) Journal of Physics: Conference Series

5. Iskandarov S.Q, A.B.Mavlanov."ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ". 2023