АСИММЕТРИК АЛГОРИТМЛАРНИ ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА ЎТКАЗИШ МАСАЛАЛАРИ

Матякубов Алишер Самандарович
Ўзбекистон Миллий университети, 7430123@gmail.com
Алимжанова Диёра Азамат қизи
ЎзМУ 1-курс магистратура талабаси

Агар замонавий асимметрик алгоритмлар математик мураккабликлари ҳисобланган факторизация ва чекли майдонда дискрет логарифмлаш масалаларини ҳал қилишнинг эффектив усуллари ишлаб чиқилса (ёки таклиф этилса), бу каби алгоритмлардан амалда фойдаланиш тавсия этилмайди ва алгоритм мураккаблигини ўзгартириш зарурати пайдо бўлади. Шу сабабдан, криптография фанида янги математик мураккаблик масалалари асосида асимметрик алгоритмлар яратишда эллиптик эгри чизиқлар деб аталувчи назария мавжуд бўлиб, ушбу ишда эллиптик эгри чизиқларга ўтказиш масалалари келтирилган.

Семаев И.А. [1] ишларида ихтиёрий чекли группа учун дискрет логарифмлаш усуллари таклиф этилган. Курьязов Д.М. [2, 4, 5] ишларида жадвалда калит узунликлари турлича бўлганда замонавий компьютерлар ҳисоблаш имкониятларидан келиб чиқиб факторизация, чекли майдонда дискрет логарифмлаш ва эллиптик эгри чизиқда дискрет логарифмлаш масалаларини таҳлил қилиш муракабликлари келтирилган.

Бугунги кунда аксарият асимметрик шифрлаш алгоритмлар мураккаблиги чекли майдонда дискрет логарифмлаш масаласига асосланган бўлиб, ушбу алгоритмларни эллиптик эгри чизиқларга ўтказиш масаласи алоҳида изланиш талаб этади. Факторизация, чекли майдонда дискрет логарифмлаш мураккабликларга нисбатан кичик узунликдаги параметрларда эллиптик эгри чизиқга асосланган бардошли асимметрик алгоритмлар яратиш мумкин.

Қуйидаги тушунчаларни киритамиз.

Таъриф. Агар n мусбат бутун сон учун қуйидаги каноник $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_s^{\alpha_s}$ ёйилмани топиш масаласи қаралаётган бўлса, у ҳолда бундай масала берилган n мураккаб сонни туб кўпайтувчиларга ажратиш (ёки факторизация) дейилади. Бу ерда p_i жуфт-жуфти билан турли туб сонлар, $\alpha_i \geq 1$.

Амалда, хусусан криптология фанида $n = p*q$ сонни туб кўпайтувчиларга ажратиш масаласи қаралади. Шунинг учун кейинги баёнларда туб кўпайтувчиларга ажратиш (ёки факторизация) масаласи ҳақида фикр юритилганда айнан мазкур ҳолат назарда тутилади.

Таъриф. Агар берилган a, b бутун, p-туб ва $1 < a, b < p$ сонлар учун $a^x \equiv b(mod\ p)$ таққослама тенглама x бутун ечимини топиш масаласи қаралаётган

бўлса, у ҳолда бундай масала F_p чекли майдонда дискрет логарифмлаш масаласи деб аталади.

Таъриф. Берилган $y^2 = x^3+ax+b(\text{mod } p)$ эллиптик эгри чизиқ **(**ЭЭЧ) ва унга тегишли $G(x_1,y_1)$ базавий нуқта учун $[d]G(x_1,y_1) = Q(x_2,y_2)$ тенгликдан d сонини топиш ЭЭЧ группасида дискрет логарифмлаш масаласи дейилади.

Бу ерда a, b фиксирланган элементлар, p-етарлича катта туб сон, $0 < d < n$, $[n]G(x_1,y_1) = 0$ бўлиб, n – сони $G(x_1,y_1)$ базавий нуқтанинг тартиби, $Q(x_2,y_2)$ очиқ калит, d - эса ёпиқ калит ҳисобланади.

Эллиптик эгри чизиқлар ва улар билан боғлиқ тушунчалар

Агар замонавий асимметрик алгоритмлар математик мураккабликлари ҳисобланган факторизация ва чекли майдонда дискрет логарифмлаш масалаларини ҳал қилишнинг эффектив усуллари ишлаб чиқилса (ёки таклиф этилса), бу каби алгоритмлардан амалда фойдаланиш тавсия этилмайди ва алгоритм мураккаблигини ўзгартириш зарурати пайдо бўлади. У ҳолда мазкур масала ўз навбатида қуйидаги учта муаммони келтириб чиқаради:

1. Параметрларга қўйилган талабларни ўзгартириш, яъни алгоритмларда фойдаланилган сонлар разрядини ошириш. Бироқ бу ҳолат алгоритм ишлаш тезлигининг сезиларли даражада пасайишига олиб келади.
2. Асимметрик алгоритмнинг бир вақтда факторизация ва дискрет логарифмлаш математик мураккабликлари комбинациялари орқали янги вариантларини ишлаб чиқиш.
3. Алгоритмларда фойдаланилган бир томонли функцияларни ўзгартириш, яъни математик мураккабликни бошқа янги мураккабликка ўтказиш. Мураккаблик шундан иборат бўлиши керакки, етарлича кичик узунликдаги сонлар билан амалий нуқтаи назаридан тегишли бардошлиликни таъминласин.

ElGamal асимметрик шифрлаш алгоритмини эллиптик эгри чизиқларга ўтказиш

Қуйида чекли майдонда дискрет логарифмлаш мураккаблига асосланган ElGamal асимметрик шифрлаш алгоритмини эллиптик эгри чизиқларга ўтказиш масаласи келтирилган [2, 6]

ElGamal шифрлаш алгоритми	ЭЭЧ мураккаблигига ўтказилган ElGamal шифрлаш алгоритми
Алгоритм параметрларини генерация қилиш	
1. Юқори тартибдаги туб сон ***p*** аниқланади. **2.** ***p*** туб сонидан кичик g, x бутун сонларини танланади. **3.** x ёпиқ калит.	**1.** Танланган $y = x^3 + ax + b(mod\ p)$ учун ***p*** тартиби аниқланади. **2.** ЭЭЧ га тегишли бўлган $G(x_0, y_0)$, базавий нуқта топилади.

4. $y = g^x\ (modp)$ ҳисобланиб очиқ калит топилади. **5.** $k < \boldsymbol{p}$ ва ЭКУБ$(k, p-1) = 1$ шартни қаноатлантирувчи сон танланади.	**3.** $0 < d < p-1$ шарт билан ёпиқ калит танланади. **4.** $Q = [d]G(x_0, y_0)$ ҳисобланиб, очиқ калит топилади. **5.** $0 < k < p-1$ ихтиёрий сон танланади.
Шифрлаш жараёни	
1. Шифрланувчи маълумот ***M.*** **2.** $a = g^k modp$ ифодани ҳисоблаш. **3.** $b = (M \cdot y^k) modp$ ифодани ҳисоблаш. **4.** (a, b) шифр маълумот.	**1.** Шифрланувчи маълумот ***M.*** **2.** $a = [k]G(x_0, y_0)$ ифодани ҳисоблаш. **3.** $b = [k]Q(x_0, y_0) \cdot M$ ифодани ҳисоблаш. **4.** (a, b) шифр маълумот.
Шифрни очиш жараёни	
1. $M = (\frac{b}{a^x}) modp$ ифодани ҳисоблаш ва очиқ матнга эга бўлиш.	1. $M = (\frac{b}{[x]a}) mod\ p$ ифодани ҳисоблаш ва очиқ матнга эга бўлиш.
Алгоритмнинг корректлиги	
$M = \frac{b}{a^x} \equiv \frac{y^k M}{a^x} \equiv \frac{g^{xk} M}{g^x k} \equiv$ $\equiv M(modp) = M.$	$M = \frac{b}{[x]a}(mod\ p) \equiv \frac{[k]Q \cdot M}{[x]a} \equiv$ $\equiv \frac{[k][x]G \cdot M}{[x][k]G} = M.$

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР:

1. Semaev, I. A. On computing logarithms on elliptic curves. Discrete Math. Appl. 6, No. 1, 69-76 (1996).

2. Курьязов Д.М. Асимметричный алгоритм шифрование данных на эллиптической кривой. Вестник Ташкентского университета информационных технологий, №2, 2014г., стр. 56-62.

3. Болотов А.А. и др. Элементарное введение в эллиптической криптографии: алгебраические и алгоритмические основы. Москва, МЭИ, 2006.- 328 с.

4. Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves // International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. №1, 2020, India, pp.295-298.

5. Kuryazov D.M. Optimal asymmetric data encryption algorithm // Global Journal of Computer Science and Technology, volume 21 Issue 2, 2021., pp. 29-33.

6. Matyakubov A.S., Berdikhobilova F. Mathematical foundations of the transfer of the El-Gamal asymmetric encryption algorithm to elliptic curves. International Journal of Education, Social Science & Humanities. FARS Publishers. Volume-11, Issue-2, 2023. P.225-229.