UDK. 004.056.57

Amirkulov Ch.J.
O'qituvchi, Termiz davlat universiteti
Termiz

Annotatsiya: *Classic McEliece algoritmi kodga asoslangan kriptografiya sohasida uzoq vaqt sinovdan o'tgan algoritm bo'lib, sindromni dekodlash muammosiga asoslanadi. Maqola algoritmning matematik asoslari, kalit generatsiyasi, shifrlash va deshifrlash jarayonlarini batafsil yoritadi, shuningdek, xavfsizlik tahlili va amaliy qo'llanilishini muhokama qiladi.*

Kalit so'zlar*: Classic McEliece, post-kvant kriptografiyasi, Goppa kodlari, sindromni dekodlash, shifrlash, kvant chidamliligi.*

Amirkulov Ch.J.
lecturer, Termiz state university
Termiz

CLASSIC MCELIECE ALGORITHM: CODE-BASED ENCRYPTION IN POST-QUANTUM CRYPTOGRAPHY

Abstract: *The Classic McEliece algorithm is a time-tested code-based cryptographic algorithm that relies on the syndrome decoding problem. This article provides a detailed explanation of the algorithm's mathematical foundations, key generation, encryption, and decryption processes, as well as an analysis of its security and practical applications.*

Keywords*: Classic McEliece, post-quantum cryptography, Goppa codes, syndrome decoding, encryption, quantum resistance.*

Kirish

So'nggi o'n yilliklarda kvant kompyuterlari sohasidagi yutuqlar an'anaviy kriptografik tizimlarga jiddiy xavf solmoqda. Post-kvant kriptografiyasi (PQC) bu muammolarni hal qilish uchun kvant va klassik hujumlarga chidamli algoritmlarni ishlab chiqishga qaratilgan. PQC algoritmlari turli matematik

muammolarga asoslanadi, masalan, lattis muammolari, sindromni dekodlash va hash funktsiyalari.

Kvant kompyuterlarining rivojlanishi an'anaviy umumiy kalitli shifrlash tizimlariga, masalan, RSA va ECC (Elliptic Curve Cryptography) algoritmlariga jiddiy xavf tug'dirmoqda. Shor algoritmi diskret logarifm va faktorizatsiya muammolarini polinomial vaqtda yechish imkonini beradi, bu esa an'anaviy shifrlash tizimlarini zaiflashtiradi. [1]Shu sababli, post-kvant kriptografiyasi sohasi faol rivojlanmoqda, unda kvant hujumlariga chidamli algoritmlar ishlab chiqilmoqda. Classic McEliece algoritmi, 1978-yilda Robert McEliece tomonidan taklif qilingan, kodga asoslangan kriptografiya sohasida muhim o'rin tutadi. U binar Goppa kodlariga asoslanib, sindromni dekodlash muammosining NP-complete murakkabligidan foydalanadi. Bu xususiyati uni post-kvant kriptografiyasida eng ishonchli algoritmlardan biriga aylantiradi.

Matematik asoslari

• **Goppa kodlari:** Goppa kodlari $GF(2^m)$ Galua maydonida aniqlangan xatolar tuzatish kodlari bo'lib, quyidagi parametrlarga ega:

– Uzunlik: $n=2^m$,

– O'lcham: $k \geq n-mt$,

– Xato tuzatish qobiliyati:t.[2]

Goppa kodlari xato tuzatishda yuqori samaradorlikka ega bo'lib, Classic McEliece algoritmining asosini tashkil qiladi.

• **Sindromni dekodlash:** Berilgan H tekshiruv matritsasi va sindrom $s=He^T$ uchun og'irligi $\leq t$ bo'lgan e xato vektorini topish muammosi. Bu muammo NP-complete sifatida tasniflanadi va kvant kompyuterlari uchun ham yechimi qiyin hisoblanadi.

[1] Amirkulov Ch.J., Normurodov Ch.B. (2020). *Навье – Стокс тенгламаларининг айрим хусусий ечимлари ҳақида*. Интернаука, 4(16)

[2] Kholyorov Erkin, Turayev Dilmurod, Buriyev Javokhir (2024). *Numerical solution of boundary inverse problem for fluid relaxation filtration in porous media*. AIP Conference Proceedings, https://doi.org/10.1063/5.0241626.

• **Parametrlar:** Masalan, m = 12, n = 4096, t = 128 kabi parametrlar 256-bit xavfsizlik darajasini ta’minlaydi, bu esa zamonaviy xavfsizlik talablariga mos keladi.

Algoritm tuzish

1. Kalit generatsiyasi:

• Tasodifiy $g(x)$ Goppa polinomi (darajasi t) tanlanadi.

• G generatsiya matritsasi Goppa kodi asosida yaratiladi.

• Maxfiy kalit: $(S, g(x), P)$, bu erda $S - k \times k$ invertalanadigan matritsa, $P - n \times n$ almashinuv matritsasi.

• Umumiykalit: $G' = SGP$, bu erda G' umumiy kalit sifatida nashr qilinadi.

2. Shifrlash:

• Xabar m (uzunligi k-bit) va tasodifiy xato vektori e (og‘irligi $\leq t$) tanlanadi.

• Shifrlangan matn: $c = mG' + e$.[3]

3. Deshifrlash:

• $c\,P^{-1}$ hisoblanadi.

• Goppadekodlash algoritmi (masalan, Patterson algoritmi) yordamida mS olinadi.

• Asl xabar $m = (mS)S^{-1}$ orqali tiklanadi[4].

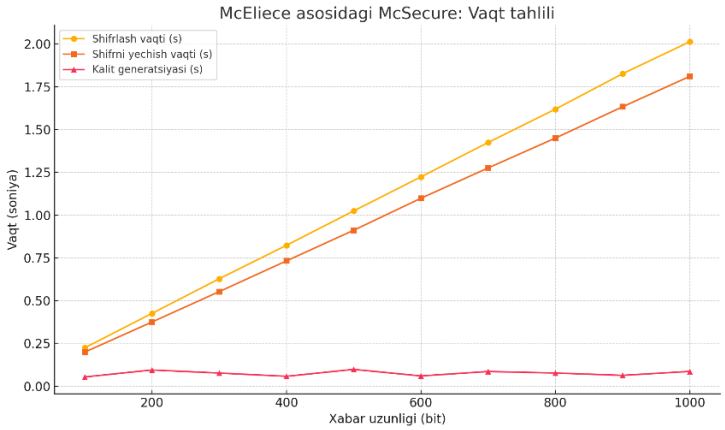
Natijalar

• Xavfsizlik: Classic McEliece algoritmi sindromni dekodlash muammosiga asoslangan xavfsizligi kvant hujumlariga chidamli. Grover

[3] Normurodov Chori Begaliyevich, Turaev Dilmurod Shokirovich, Jabborov Ilyor Yuldashevich, Buriev Javoxir Nosirovich, Jonqobilov Mirjalol Bakhtiyorovich (2021). *Definition of Different Schemes for Calculation of General Solutions*. Nashr ma'lumotlari aniq emas (konferensiya yoki jurnal ma'lumotlari keltirilmagan).

[4] Kholyorov Erkin, Turayev Dilmurod, Buriyev Javokhir (2024). *Численное решение граничной обратной задачи для уравнения релаксационной фильтрации*. Проблемы вычислительной и прикладной математики

algoritmi qidiruvni kvadrat ildiz darajasida tezlashtirsada, katta parametrlar (masalan, n = 4096,t = 128) xavfsizlikni ta’minlaydi.



1-rasm. Algoritm taxliliy natijalari

• Samaradorlik: Shifrlash jarayoni(matritsa ko‘paytirish) va deshifrlash (Goppa dekodlash) yuqori tezlikda amalga oshiriladi.

• Amaliy qo‘llanilishi: Algoritm uzoqmuddatli ma’lumotlar himoyasi(masalan, maxfiy hujjatlar, davlat tizimlari) va maxfiy aloqa tarmoqlari uchun ideal.

• Cheklovlar: Umumiy kalit o‘lchami(1MB) katta bo‘lib, bu IoT kabi resursi cheklangan muhitlarda qo‘llanilishini qiyinlashtiradi.

Tahlil

• **Xavfsizlik tahlili:** Algoritmning xavfsizligi sindromni dekodlash muammosining matematik murakkabligiga asoslanadi. Eng samarali hujum Information Set Decoding (ISD)– katta hisoblash resurslarini talab qiladi.

• **Samaradorlik tahlili:** Algoritmning shifrlash va deshifrlash jarayonlari o‘ta samarali bo‘lib, matritsa ko‘paytirish va Goppa dekodlash algoritmlari minimal hisoblash resurslarini talab qiladi.

• **Taqqoslash:** CRYSTALS-Kyber va CRYSTALS-Dilithium kabi lattisga asoslangan algoritmlar kichikroq kalit o‘lchamlari bilan raqobatlashadi.

Foydalanilgan adabiyotlar

1. Bernstein, D. J., Lange, T.,Peters, C. (2008). *Attacking and defending the McEliece cryptosystem*. International Workshop on Post-Quantum Cryptography (PQCrypto 2008).
2. McEliece, R. J. (1978). *A public-key cryptosystem based on algebraic coding theory*. DSN Progress Report, Jet Propulsion Laboratory, California Institute of Technology.
3. Fouque, P.A., Joux, A., Mavromati, C. (2020). *SQISign: Compact post-quantum signatures from quaternions and isogenies*. International Association for Cryptologic Research.
4. Aumasson, J.-P., Bernstein, D. J. (2019). *SPHINCS+: Stateless hash-based signatures*. NIST Post-Quantum Cryptography Standardization Project, Round 3 Submission.
5. Normurodov Chori Begaliyevich, Turaev Dilmurod Shokirovich, Jabborov Ilyor Yuldashevich, Buriev Javoxir Nosirovich, Jonqobilov Mirjalol Bakhtiyorovich (2021). *Definition of Different Schemes for Calculation of General Solutions*. Nashr ma'lumotlari aniq emas (konferensiya yoki jurnal ma'lumotlari keltirilmagan).
6. Buriyev J. N. (2024). *WINDOWS FORMS .NET ILOVALARNING DIZAYNIDA UI/UX FRAMEWORKLARINING AFZALLIKLARI*. Ekonomika va Sotsium Jurnali.
7. Kholyorov Erkin, Turayev Dilmurod, Buriyev Javokhir (2024). *Numerical solution of boundary inverse problem for fluid relaxation filtration in porous media*. AIP Conference Proceedings, https://doi.org/10.1063/5.0241626.
8. Kholyorov Erkin, Turayev Dilmurod, Buriyev Javokhir (2024). *Численное решение граничной обратной задачи для уравнения релаксационной фильтрации*. Проблемы вычислительной и прикладной математики

9. Normurodov Chori Begaliyevich, Toyirov Akbar Khasanovich, Amirkulov Chori Jumayevich, Abdullaev Bakhtiyor Panji O'g'li (2020). *Mathematical Modeling of the Hydrodynamic Stability Problem by the Spectral-grid Method*. International Journal of Innovations in Engineering Research and Technology.