# SIMMETRIK UZLUKSIZ SHIFRLASH ALGORITMLARI KRIPTOBARDOSHLILIGINI BAHOLASH MEZONLARI

*Rahmatullayev Ilhom Raxmatullayevich*

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali dotsenti*
*E-mail: Ilhom9001@gmail.com*

*K E Y W O R D S*

Kriptografik algoritmning bardoshliligi, entropiya, oqimli shifrlash, moslashuvchanlik hujumi, “bo‘lib tashla va egalik qil” hujumi

*A B S T R A C T*

Ushbu maqolada shifrlash algoritmlarining bardoshliligi masalalari, oqimli shifrlash nazariyasi va oqimli shifrlash algoritmlariga nisbatan qo‘llaniladigan ayrim kriptotahlil usullari ko‘rib chiqiladi. Maqolada asosiy e'tibor moslashuvchanlik va “bo‘lib tashla va egalik qil” hujumlari kabi muhim tahlil usullariga qaratilgan. Ushbu hujumlar sodda misollar bilan yoritilib, oqimli shifrlash algoritmlarining bardoshliligini baholashda qanday qo‘llanilishi tushuntiriladi. Maqola oqimli shifrlash algoritmlarining xavfsizligini oshirish yo‘llarini o‘rganish va ularning zaif tomonlarini aniqlash maqsadida yozilgan.

## Kirish

Kriptografik algoritmning bardoshliligi uning kriptotahlilchi tomonidan buzilishi yoki zaif tomonlarining topilishi uchun zarur bo‘lgan hisob-kitoblar yoki resurslarning umumiy miqdori bilan o‘lchanadi. Bu bardoshlilik ko‘pincha algoritmning hisoblash murakkabligi orqali ifodalanadi. Hisoblash murakkabligi — bu algoritmning buzilishini imkonsiz yoki nihoyatda qiyin qiladigan hisoblash quvvatini talab qiluvchi daraja. Kriptografik algoritmning bardoshliligi qanchalik yuqori bo‘lsa, shuncha kam ehtimol bilan hujumchining kalitni yoki shifrlangan ochiq matnni tiklashi mumkin bo‘ladi [1].

Mukammal himoyalangan shifrlash algoritmi uchun hisoblash murakkabligi kalit maydoni bilan bir xil bo‘lib, bu ba’zan kalitning entropiyasi deb ham ataladi. Kalit maydoni barcha mumkin bo‘lgan kalitlarning to‘plamiga ishora qiladi va bu kalitlarning umumiy sonini ifodalaydi. Boshqacha aytganda, kalit maydoni barcha maxfiy kalit bitlari yordamida yaratib bo‘ladigan kombinatsiyalarning umumiy miqdorini bildiradi. Mukammal himoyalangan algoritmda barcha kalitlar teng ehtimollikda tanlanadi, bu esa hujumchiga barcha mumkin bo‘lgan kalitlarni sinab ko‘rishdan boshqa imkoniyat bermaydi, bu esa hisoblash murakkabligini maksimal darajada oshiradi.Kalitning o‘lchami (kalit o‘lchami) - bu to‘liq kalit maydonining hajmini ($2^n$) ifodalaydigan $n$ bitlar miqdori [2].

Maxfiy kalitni tiklashning eng sodda usuli barcha mumkin bo‘lgan kombinatsiyalarni sinab ko‘rishdir. Ushbu metodologiya ko‘pincha “to‘liq qidiruv” yoki “qo‘pol kuch hujumi” (brute force attack) deb ataladi. Bu hujumda hujumchi maxfiy kalitni aniqlash uchun deyarli $2^n$ ta variantni sinab ko‘rishi kerak, bu yerda n kalit uzunligini bildiradi. Aniqroq qilib aytganda, o‘rtacha hisobda hujumchi barcha mumkin bo‘lgan kombinatsiyalarning yarmida to‘g‘ri kalitni topishi mumkin. Shunga qaramay, hujumchi to‘g‘ri kalitni topish uchun barcha kombinatsiyalarni sinab ko‘rishi ham mumkin. Bu usulning samaradorligi kalitning uzunligiga va hisoblash resurslariga bog‘liq bo‘lib, kalit uzunligi oshgani sari hujumning muvaffaqiyat ehtimoli kamayadi [3].

Mukammal xavfsiz bo‘lgan shifrlash usuli xavfsiz kriptotizimning asosi bo‘lishi kerak. Amalda esa, ko‘pchilik shifrlash algoritmlari o‘zlarining maxfiy kalitlarining to‘liq entropiyasidan zaifroq bo‘ladi. Bunday algoritmlar

©Rahmatullayev Ilhom Raxmatullayevich

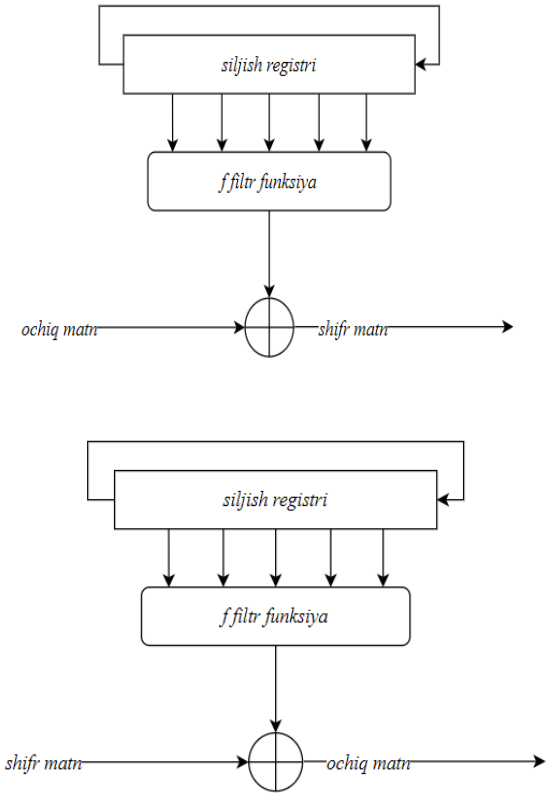
zaiflikka ega bo‘lib, bu zaifliklardan foydalangan holda hisob-kitoblarni optimallashtirish orqali haqiqiy entropiyadan kamroq hisob-kitoblarni amalga oshirish orqali maxfiy kalitni topish mumkin. Bu shifrning “haqiqiy hujum murakkabligi” deb ataladi. Haqiqiy hujum murakkabligi shifrning nazariy xavfsizligidan past bo‘lishi mumkin, chunki tahlilchilar ma’lum bir usullardan foydalangan holda hisob-kitoblarni soddalashtirish yoki qisqartirishga muvaffaq bo‘lishadi [4].

*Oqimli shiflash algoritmlari*

Oqim shifrlash bir martalik bloknot (One-Time Pad, OTP) shifrlash texnikasiga o‘xshash shifrlashni amalga oshiradi. U maxfiy, tasodifiy ko‘rinadigan ma’lumotlarning katta qismini ishlab chiqaradi va ularni shifrlangan matnni yaratish uchun ochiq matn bilan birlashtiradi. Buning natijasida, ochiq matnni shifrlangan matndan ajratib bo‘lmaydi. Bu tasodifiy ma’lumotlar maxfiy kalitdan olingan bo‘lib, odatda “kalit oqimi” deb ataladigan bitlar oqimini ifodalaydi. Oqimli shifrlash algoritmlarida maxfiy kalit tomonidan ishga tushiriladigan va har bir shifrlash bosqichidan so‘ng keyingi holatga o‘tadigan doimiy xotira mavjud bo‘lib, bu “ichki shifr holati” deb nomlanadi. Bardoshli oqimli shifrlash algoritmlarining chiqishi Pseudo Random Number Generator (PRNG) tomonidan ishlab chiqarilgan bitlar oqimi bilan taqqoslanadi. PRNG shifrlash uchun zarur bo‘lgan tasodifiylikni ta’minlaydi va algoritmning xavfsizligi ushbu tasodifiylikning sifatiga bog‘liq [5].

Oqimli shifrlash algoritmlarini ishlab chiqishda foydalaniladigan eng mashhur usullardan biri chiziqli bo‘lmagan ikkilik ketma-ketliklarni ishlab chiquvchi generatorlardan foydalanishdir. Ushbu generatorlar ikkilik kalitlar oqimini ishlab chiqaradi, bu esa juda katta maxfiy kalitni talab qilmasdan muntazam bir martalik shifrlash imkonini beradi. Chiziqli bo‘lmagan ketma-ketliklar shifrning tasodifiyligini va kriptografik xavfsizligini ta’minlashda muhim ahamiyatga ega. Bunday generatorlar shifrlash jarayonida katta tasodifiylik darajasini ta’minlab, ochiq matnning shifrlangan matndan ajralishini imkonsiz qiladi [6].

Chiziqli bo‘lmagan oqim shifri asosidagi odatiy kriptotizimning umumiy ko‘rinishi 1-rasmda tasvirlangan. Ushbu turdagi shifrlar kichik apparat ko‘rinishida amalga oshirish imkoniyati sababli juda mashhurdir. Kichik apparat talab qiladigan shifrlar resurs cheklangan muhitlarda, masalan, o‘rnatilgan tizimlar yoki mobil qurilmalarda, samarali ishlash imkonini beradi. Chiziqli bo‘lmagan ketma-ketliklar yuqori darajadagi tasodifiylikni ta’minlab, shifrlash algoritmining xavfsizligini oshiradi va hujumchilarning kalitni tiklashini qiyinlashtiradi.




*1-rasm. Oddiy chiziqsiz oqimli shifrlash tizimi sxemasi*

1-rasmda ko‘rsatilgan kriptografik algoritm shifrning ichki holatini ifodalovchi aylanuvchi siljish registrini o‘z ichiga oladi. Bu registr kalit oqimini yaratishda asosiy rol o‘ynaydi. Kalitning har bir bitini hisoblashdan so‘ng, ichki holat chiziqli funksiya yordamida yangilanadi, bu funksiya ichki holatda ko‘proq entropiyani saqlab qolish va shifrlash jarayonining xavfsizligini ta’minlash maqsadida ishlatiladi. Chiziqli bo‘lmagan funksiya shifrni kriptotahlilga nisbatan bardoshlilik

©Rahmatullayev Ilhom Raxmatullayevich

darajasini oshiradi, chunki u shifrning ichki tuzilishini tushunishni va kalitni tiklashni qiyinlashtiradi. Chiqish komponenti keyingi kalit oqimi bitini hisoblash uchun chiziqli bo‘lmagan $f(\cdot)$ filtr funksiyasini qo‘llaydi. Kalit oqim bitlari $XOR$ ($\oplus$) operatsiyasi bilan, jo‘natuvchi tomonidan ochiq matn bitlarini shifrlash uchun ishlatiladi. Olingan shifrlangan matn xavfsiz bo‘lmagan kanal orqali uzatiladi. Qabul qiluvchi aynan bir xil hisob-kitoblarni amalga oshiradi va kalit oqimi bitlari bilan birgalikda shifrlangan matn bitlaridan ochiq matnni hosil qilish uchun $XOR$ operatsiyasini qo‘llaydi. Shifrlangan matnga allaqachon kiritilgan kalit oqimi bitlari bekor qilinadi va qabul qiluvchida ko‘rinadi asl ochiq matn bitlari hosil bo‘ladi [7].

Adabiyotlarda oqimli shifrlash algoritmlariga nisbatan kriptografik hujumlarda qo‘llaniladigan ko‘plab ilg‘or va murakkab kriptotahlil metodologiyalari va usullari taklif qilingan. Ushbu maqolada oqimli shifrlash algoritmiga nisbatan kriptotahlil usullarining qo‘llanilish texnikalari yoritilgan. Maqola kriptotahlilning turli xil yondashuvlari, jumladan, statistik tahlil, differensial kriptotahlil, va boshqa murakkab usullarni ko‘rib chiqadi. Ushbu usullar shifrning zaif tomonlarini aniqlash va uni buzish imkoniyatlarini o‘rganishda muhimdir. Kriptotahlilning samarali usullari oqimli shifrlash algoritmlarini takomillashtirish va ularning xavfsizligini oshirishda katta ahamiyatga ega.

## Asosiy qism

Kriptografik hujum uchun zarur bo‘lgan hisob-kitoblarni (qisman) oldindan hisoblash mumkin bo‘lgan tarzda umumlashtirish mumkin. Bunday texnika odatda Time-Memory Trade-Off (TMTO) deb ataladi. TMTO texnikasi kriptografik hujumni ikki bosqichga, hisoblashdan oldingi bosqichga (off-line) va faol hujum bosqichiga (onlayn) bo‘lish prinsipiga asoslanadi [8].

TMTO usuli umumiy g‘oyasi hisob-kitoblarni oldindan (off-line) tayyorlab, ularni keyinchalik faol hujum bosqichida (onlayn) tezroq foydalanishga imkon beradi. Bu usulda, katta miqdorda hisoblash ishlari oldindan bajariladi va natijalar saqlanadi. Faol hujum bosqichida, bu oldindan hisoblangan natijalar yordamida hujumni tezlashtirish mumkin.

Batafsil ma’lumotlarni [9-11] adabiyotlarda taklif qilingan TMTO usullari va samarali qidiruv usullaridan olish mumkin. Ushbu usullar kriptografik xavfsizlikni oshirish va zaifliklarni kamaytirishda yordam beradi.

*Moslashuvchanlik hujumi*

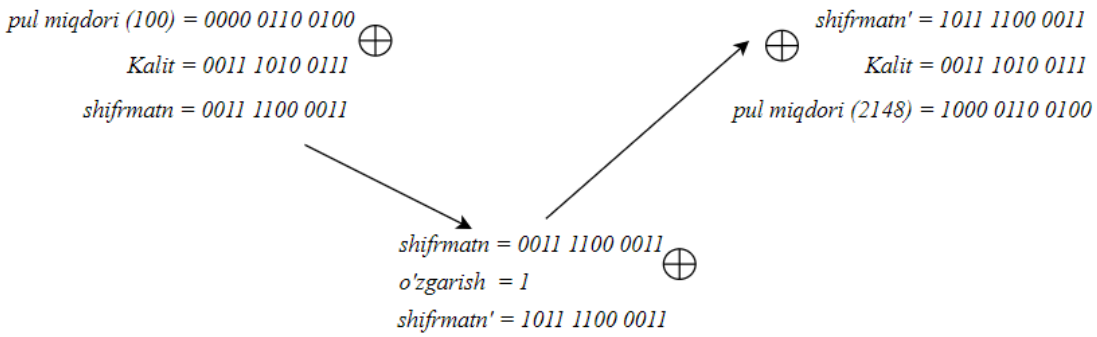
Chiziqli bo‘lmagan ikkilik ketma-ketlikni hosil qiluvchi sinxron oqimli shifrlash algoritmi ikkilik ketma-ketlikni kalit oqimi sifatida ishlatadi va XOR operatori yordamida ochiq matn bilan birlashtiriladi. Bunday kriptotizim odatda ma’lumotlarni uzatishning maxfiyligini himoya qilish uchun xavfsiz kanalni ta’minlaydi. Ammo, bu tizim qo‘shimcha ravishda ma’lumotlarning yaxlitligini kafolatlamaydi.

Ma’lumotlarning haqiqiyligini himoya qilish uchun qo‘shimcha choralar, masalan, Xabar autentifikatsiya kodi (MAC) kabi kriptografik usullarni qo‘llash zarur. Qo‘shimcha kriptografik usulsiz oqimli shifrlash tizimi moslashuvchanlik hujumlariga nisbatan bardoshsiz bo‘lishi mumkin, chunki bu hujumlar ma’lumotlarning yaxlitligini buzishi yoki o‘zgartirilgan ma’lumotni haqiqiy deb qabul qilish imkonini beradi [12].

Moslashuvchanlik hujumining maqsadi maxfiy kalitni tiklash emas, balki kriptotizimning xavfsizligini buzishga urinishdir, hatto maxfiy kalit haqida hech qanday ma’lumotga ega bo‘lmasdan ham. Bunday hujumlar kriptotizimning boshqa zaif tomonlarini aniqlash va undan foydalanishga qaratilgan.

2-rasmda moslashuvchanlik hujumi uchun zaif bo‘lgan bank ilovasining ma’lumotlar uzatish tizimining buzilishi ko‘rsatilgan. Bu holatda, kichik pul o‘tkazmasini ifodalovchi ketma-ketlikdagi bir bitni o‘zgartirish orqali to‘satdan juda katta pul o‘tkazmasini ifodalashga erishiladi. Bu misol kriptotizimning boshqa komponentlari, masalan, ma’lumotlar yaxlitligini tekshirish yoki autentifikatsiya, zaif bo‘lishi mumkinligini ko‘rsatadi [13].

©Rahmatullayev Ilhom Raxmatullayevich




*2-rasm. Moslashuvchanlik hujumida pul o'tkazmasi qiymatini o'zgartirish jarayoni*

Agar kalit oqimi o'ta xavfsiz oqimli shifrlash algoritmida ishlab chiqarilgan bo'lsa ham, boshqa komponentlar, masalan, ma'lumotlarning yaxlitligini ta'minlovchi qo'shimcha mexanizmlar hali ham zaif bo'lishi mumkin. Bu holatda, haqiqiy xavfsizlik kriptotizimning butun bardoshliligi va uning barcha komponentlarining xavfsizligi orqali ta'minlanadi.

Moslashuvchanlik hujumi samarali bo'lishi mumkin, ammo uni qo'llash oson emas. Buzg'unchi, pulning qayerda va qachon uzatilishini aniq bilishi kerak, chunki noto'g'ri pozitsiyada bitni o'zgartirish ma'nosiz bo'lishi va uzatishning buzilishiga olib kelishi mumkin.

Kalitlar oqimi haqidagi bilimlar buzg'unchiga yanada puxta ishlab chiqilgan hujumlarni tayyorlash imkonini beradi. Bu, asosan, kalit oqimidan qayta foydalanishni o'z ichiga oladi, bu esa kalitning bir nechta ma'lumot to'plamida ishlatilishiga olib keladi. Shuning uchun, ikkilik ketma-ketlik faqat bir marta ishlatilishi juda muhimdir.

Oqimli shifrdan har safar foydalanilganda ichki holat takrorlanmas qiymat bilan ishga tushirilishi kerak. Bu, shifrlashning xavfsizligini oshiradi va kalit oqimini bir marta ishlatish prinsipiga rioya qilish orqali moslashuvchanlik hujumlarining samaradorligini kamaytiradi. Har safar yangi va tasodifiy ichki holat yaratilishi, shifrlash tizimining mustahkamligini ta'minlashga yordam beradi[14].

*"Bo'lib tashla va egalik qil" hujumi*

Hisoblashning murakkabligini kamaytirishning eng samarali usullaridan biri bitta katta muammoni ikkita alohida kichik masalalarga bo'lishdir, bu usul ko'pincha "bo'lib tashla va egalik qil" (Divide and Conquer) deb ataladi. Bu usul turli sohalarda, shu jumladan kriptografiya, qiyin hisoblash masalalarini yechishni optimallashtirish uchun ishlatiladi [15].

"Bo'lib tashla va egalik qil" usulining asosiy maqsadi hisoblash murakkabligini kamaytirish va umumiy qo'llanilishni optimallashtirishdir. Kriptotizimlarda bu usul ayniqsa foydalidir, chunki u murakkab hujumlarni boshqarish va ularning samaradorligini oshirish uchun ideal hisoblanadi. Ushbu metodologiya orqali katta muammolarni kichikroq, boshqarish osonroq bo'lgan masalalarga bo'lib, yechimini topish ancha soddaroq bo'ladi. Bu kriptografik tizimlarda murakkab hisoblash jarayonlarini optimallashtirishga yordam beradi va xavfsizlikni oshiradi [16].

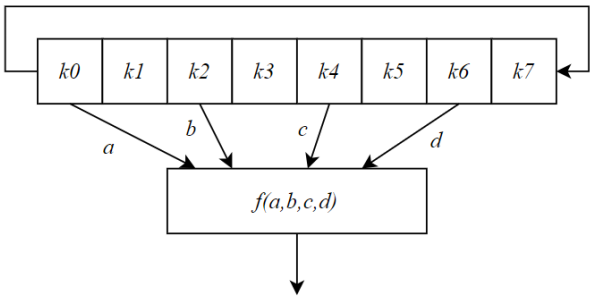
Muammolarni bo'lish orqali murakkablikni kamaytirish, masalan, 80 bit uzunlikdagi maxfiy kalitga ega kriptografik himoyalangan shifrni ochish uchun juda ko'p vaqt va resurslar talab qilinishi mumkin. Bunday shifrlash tizimi uchun to'liq qidiruvni bo'lish murakkablikni kamaytirmaydi. Bunday holatda, raqib faqat ikkita qidiruvni parallellashtirish imkoniyatiga ega bo'ladi, ularning har biri asosiy muammoning aniq yarim murakkabligini $2^{79}$ deb belgilaydi.

Biroq, agar tahlilchi katta muammoni ikkita kichikroq masalaga bo'lish yo'lini topsa, murakkablik sezilarli darajada kamayishi mumkin. Bu usul murakkablikni sezilarli darajada

©Rahmatullayev Ilhom Raxmatullayevich

kamaytirish imkonini beradi, chunki kichik masalalarni hal qilish katta masalani hal qilishdan ancha osonroq bo‘ladi. “Bo‘lib tashla va egalik qil” usuli, shuningdek, hisoblash resurslarini samarali ishlatishga yordam beradi va shifrlash tizimining zaif tomonlarini aniqlashni osonlashtiradi. Bu strategiya, shuningdek, hisoblashning umumiy vaqtini qisqartirish va resurslarni optimallashtirishda muhim rol o‘ynaydi.

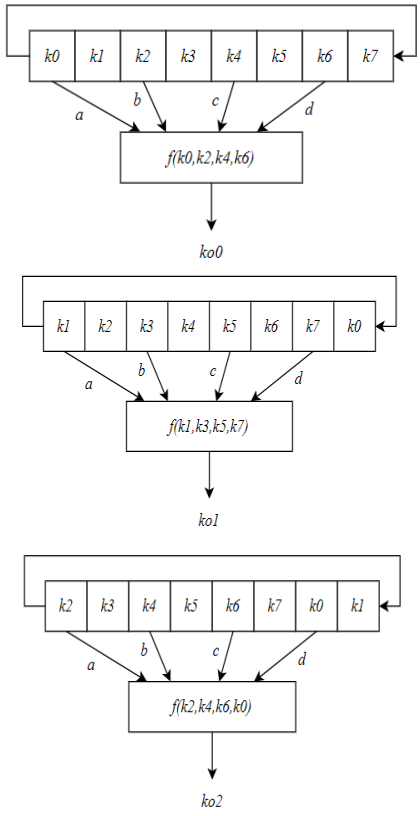
3-rasmda keltirilgan shifrlash sxemasi uchun mazkur hujumni qanday o‘tkazish mumkinligini ko‘rib chiqish mumkin. Initsializatsiya jarayonida 8 bitli maxfiy $k = k_0, k_1, \dots, k_7 \in F_2$ kalit ichki holatga yuklanadi. Ichki holatdagi har bir iteratrsiya chiqish sifatida kalit bitini ishlab chiqargandan so‘ng, bir qadam chapga suriladi. Faqat $2^8 = 256$ kalitlar oqimidan iborat shifrning kalit maydoni sakkiz marta aylanishdan keyin takrorlanadi. Shuning uchun bu algoritmni xavfsiz deb hisoblab bo‘lmaydi. Biroq, uning soddaligi ko‘rib o‘tilayotgan hujum usulining mohiyatini aks ettirish uchun mos keladi.




*3-rasm. “Bo‘lib tashla va egalik qil” hujumini ifodalash uchun foydalaniladigan algoritm sxemasi*

3-rasmda ko‘rsatilganidek oqimli shifrlash algoritmida sakkizta yacheykadan iborat siljish registri mavjud. Ushbu registrga ishga tushirish vaqtida maxfiy kalitning birlari va nollari yuklanadi. $f(\cdot)$ komponenti chiziqli bo‘lmagan funksiya bo‘lib, u 4 ta kirish bitlaridan foydalanib 1 chiqish bitini ishlab chiqaradi, bu ishlab chiqilgan bitlar ketma-ketligi - kalit oqimi $ko$ deb ataladi. $i$ – iteratsiyada ishlab chiqilgan bit esa $ko_i$ bilan belgilanadi.

4-rasmda dastlabki uchta shifrlash iteratsiyasi tasvirlangan. $ko_0, ko_1$ va $ko_2$ chiqish bitlarini ishlab chiqish uchun $f(\cdot)$ funksiyasiga kirish bitlari ham tasvirlangan. Ko‘rish mumkinki, $ko_0$ va $ko_2$ ni ishlab chiqish uchun zarur bo‘lgan maxfiy kalit bitlari bir xil bo‘ladi, garchi ular tartibda farq qilsalar ham. Birinchi kalit oqimi biti $ko_0 = f(k_0, k_2, k_4, k_6)$ va uchinchi kalit oqimi biti $ko_2 = f(k_2, k_4, k_6, k_0)$ bilan ifodalanadi.



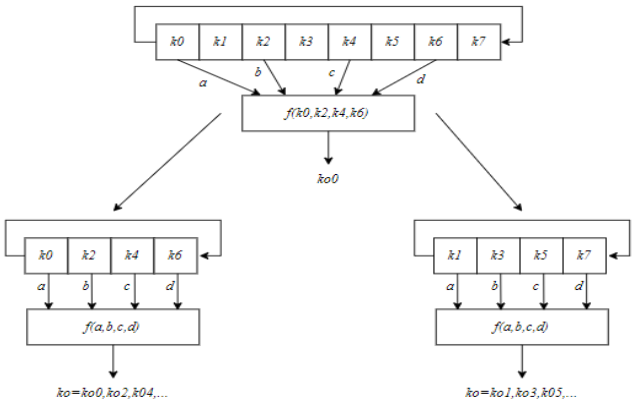

*4-rasm. Birinchi uchta shifrlash bosqichida va $ko_0$, $ko_1$ va $ko_2$ ni hisoblash jarayoni*

Chiquvchi kalit oqimidagi toq va juft tartibdagi yacheykalardan foydalanish ushbu shifrning xususiyati hisoblanadi. Juft kalitli oqim bitlarini $ks_j$ hisoblash uchun faqat $k_0, k_2, k_4, k_6$ juft kalit bitlari talab qilinsa, bunda $j \in 2N$ juft pozitsiyalarni ifodalaydi, faqat $k_0, k_2, k_4, k_6$ toq kalit bitlari toq o‘rindagi kalit oqimi bitlarini hisoblashda foydalaniladi. bit $ks_t$ bu yerda $t \in 2N$ toq pozitsiyalarni ifodalaydi.

3-rasmdagi algoritm bitta katta algoritm sifatida ishlab chiqilgan, ammo uni osonlik bilan kichikroq 2 ta algoritm bo‘lish mumkin. 5-rasmda algoritmni qismlarga qanday ajratish mumkinligi ko‘rsatilgan, ularning ikkalasining ham kalit

©Rahmatullayev Ilhom Raxmatullayevich

o'lchami asl shifrlash algoritmining kalit o'lachamining yarmiga teng.




*5-rasm. "Bo'lib tashla va egalik qil" hujumini toq va juft kalit oqim bitlariga bo'lish orqali amalga oshirish jarayoni*

Ichki shifr holatining atigi yarmi bilan toq va juft shifr uchun hisoblash murakkabligi $2^4$ ga tushadi. Shunday qilib, ikkalasi uchun umumiy murakkablik atigi $2\times2^4 = 2^5 = 32$ ga kamayadi, bu dastlabki murakkablik $2^8$=256 dan ancha kam. E'tibor bering, "bo'lib tashla va egalik qil" hujumi faqat asosiy kalit fazosining entropiyasini ikki baravar kamaytirmaydi. Bunday bo'linish murakkablikni $\frac{2^8}{2} = 2^7 = 128$ ga nisbatan ancha kichik murakkablikgacha kamaytirishga olib keladi. Shifrni ikkita mustaqil maxfiy kalitga tayanadigan ikkita kichik algoritmga ajratish ancha samaralidir, bu erda ikkita kalit asl maxfiy kalitning ikkala yarmini ifodalaydi.

## Xulosa

Mazkur maqolada shifrlash algoritmlari bardoshliligi masalalari, oqimli shifrlash nazariyasi va oqimli shifrlash algoritmlariga nisbatan qo'llaniladigan ayrim kriptotahlil usullari, xususan, moslashuvchanlik va "bo'lib tashla va egalik qil" hujumlari sodda misollar bilan yoritib berilgan. Shifrlash algoritmlarining bardoshliligi va xavfsizligi haqida muhim ma'lumotlar taqdim etilgan. Shuningdek, maqola oqimli shifrlash tizimlariga nisbatan boshqa tahlil usullarining qo'llanilishi bo'yicha keyingi tadqiqotlarda ko'rib chiqilishi kerak bo'lgan masalalarni belgilab beradi. Bu tahlil usullari kriptografik tizimlarning zaif tomonlarini aniqlash va ularning samaradorligini oshirishda yordam beradi.

## Foydalanilgan adabiyotlar

1. Whitfield Diffie and Martin E Hellman. Privacy and authentication: An introduction to cryptography. Proceedings of the IEEE, 67(3):397–427, 1979.
2. S.W. Golomb. Shift Register Sequences. Holden-Day Series in Information Systems. Holden-Day, 1967.
3. El Groth. Generation of binary sequences with controllable complexity. IEEE Transactions on Information Theory, 17(3):288–296, 1971.
4. Edwin Key. An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Transactions on Information Theory, 22(6):732–736, 1976.
5. Vera S Pless. Encryption schemes for computer confidentiality. IEEE Transactions on Computers, 100(11):1133–1136, 1977.
6. Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In 17th International Cryptology Conference, Advances in Cryptology (CRYPTO 1997), volume 1294 of Lecture Notes in Computer Science, pages 513–525. Springer-Verlag, 1997.
7. Alex Biryukov and David Wagner. Slide attacks. In 6th International Workshop on Fast Software Encryption (FSE 1999), volume 1636 of Lecture Notes in Computer Science, pages 245–259. Springer-Verlag, 1999.
8. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In 17th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT 2011), volume 7073 of Lecture Notes in Computer Science, pages 344–371. Springer-Verlag, 2011.
9. Dan Boneh, Richard A DeMillo, and Richard J Lipton. On the importance of checking cryptographic protocols for faults. In 16th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT

(cc) BY ©Rahmatullayev Ilhom Raxmatullayevich

1997), volume 1233 of Lecture Notes in Computer Science, pages 37–51. Springer-Verlag, 1997.
10. Joan Daemen, Lars Knudsen, and Vincent Rijmen. The block cipher Square. In 4th International Workshop on Fast Software Encryption (FSE 1997), volume 1267 of Lecture Notes in Computer Science, pages 149–165. Springer-Verlag, 1997.
11. Donald Davies and Sean Murphy. Pairs and triplets of DES S-boxes. Journal of Cryptology, 8(1):1–25, 1995.
12. Turakulovich X. Z., Rahmatullayevich R. I. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili //Al-Farg'oniy avlodlari. – 2024. – T. 1. – №. 1. – C. 129-134.
13. Khudoykulov Z. T., Rakhmatullayev I. R. A new key stream encryption algorithm and its cryptanalysis //Scientific and technical journal Namangan Institute of Engineering and Technology. – 2023. – T. 8. – №. 1. – C. 146-157.
14. Rakhmatullaevich R. I., Mardanokulovich I. B. Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2023. – C. 393-401.
15. Turakulovich X. Z., Rahmatullayevich R. I. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili //Al-Farg'oniy avlodlari. – 2024. – T. 1. – №. 1. – C. 129-134.
16. Rahmatullayev I. R. Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2022. – T. 2. – №. 2. – C. 119-128.

©Rahmatullayev Ilhom Raxmatullayevich