UDK 821.512.133

OQIMLI SHIFRLASH ALGORITMLARI VA ULARNI VUJUDGA KELISH SABABLARI

Rahmatullayev I.R.[1]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
ilhom9001@gmail.com

Annotatsiya. *Mazkur maqolada simmetrik shifrlash algoritmlari oilasiga mansub bo‘lgan oqimli shifrlash alogoritmlari va ularning yaratilish asoslari, shuningdek, psevdotasodifiy sonlar generatorlarining turlari va ishlab chiqish asoslari tahlil qilingan. Tizimli-nazariy yondashuv asosida yaratilgan psevdotasodifiy generatorlar, hisoblash murakkabligiga asoslangan yondashuv asosida va kombinatsiyalashga asoslangan psevdotasodifiy generatorlar va ular asosida yaratilgan oqimli sifrlash algortimlari ko‘rib o‘tilgan.*

Kalit so‘zlar: *Oqimli (uzluksiz) shifrlar, XOR, SVS, OFB, SSL, SET, LFSR, Hardware, Software, Gidrid, kombinatsion generatorlar, filtrlovchi generatorlar, vaqt nazorati generatorlari.*

I. KIRISH

Bugungi kunda oqimli (uzluksiz) shifrlar dolzarb hisoblanadi buninh asosiy sababi sifatida oqimli (uzluksiz) shifrlar blokli shifrlardan farqli ravishda axborot oqimining har bir elementi bo‘yicha shifrlab axborotning kriptotizimda ushlanib qolishiga yo‘l qo‘ymasligini aytib o‘tish muhim hisoblanadi, bu holatda uning asosiy yutug‘i axborotning miqdori, oqim razryadidan qat’iy nazar real vaqtda axborot kirish tezligiga yaqin yuqori tezlikda shifrlab kechiktirilmagan holda uzatish hisoblanadi.

Oqimli shifrlash algoritmlari simmetrik shifrlash algoritmlari oilasiga mansub bo‘lib, unda har bir ochiq matn belgisi nafaqat foydalanilgan kalitga, balki uning ochiq matn oqimidagi joylashuviga qarab shifrlangan matn belgisiga aylanadi. Oqimli shifrlashda shifrlash jarayoni blokli shifrlarga nisbatan boshqacha yondashuv asosida amalga oshiriladi [1].

II. ASOSIY QISM

Oqimli shifrlash algoritmlari gammalashga asoslangan shifrlash algoritmlari hisoblanib, ochiq matnning ketma-ket keluvchi har bir 1 bitini generator yordamida hosil qilingan mos 1 bit gamma kalitga XOR amali bilan qo‘shish orqali shifrmatnga aylantiradi [1].

$$c_i = p_i \oplus k_i \qquad (1)$$

Qabul qiluvchi olingan shifrmatndan ochiq matnni hosil qilish uchun aynan shifrlashda foydalanilgan generator yordamida (maxfiy simmetrik kalitdan foydalanib) generatsiya qilingan mos 1 bit gammaga shifrmatnni XOR bo‘yicha qo‘shadi.

$$c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i \qquad (2)$$

Oqimli shifrlashga asoslangan kriptotizimlarning turli xil hujumlarga bardoshliligi algoritmida qo‘llanilgan generatorning bardoshliligiga bog‘liq. Generatorning bardoshliligi esa, hosil

qilingan ketma-ketlikning davri va tasodifiylik darajasi bilan baholanadi. Agar generator har seansda bir xil ketma-ketlikni generatsiya qilsaaaa yoki takrorlanish davri qisqa bo‘lsa, bu orqali shifrlangan ikkita shifrmatnni XOR amali orqali qo‘shib, ikkita ochiq matnning XOR yig‘indisi $p_1 \oplus p_2$ ga ega bo‘lish mumkin. Bu shifrmatnni ochish qiyinchiligi ko‘p alfavitli shifrmatnni ochish qiyinchiligiga taxminan teng bo‘ladi, bu esa kriptohujum jarayonini osonlashtiradi.

$$p_1 \oplus k_1 = c_1, p_2 \oplus k_2 = c_2, c_1 \oplus c_2 = p1 \oplus k1 \oplus p_2 \oplus k_2 = p_1 \oplus p_2 \quad (3)$$

Oqimli shifrlash tizimlarida qo‘llaniladigan generatorlarning yana bir muhim xarakteristikasi hosil qilingan ketma-ketliklarning tasodifiylik darajasi hisoblanadi [1]. Ketma-ketliklar bloklarining tasodifiylik darajasi ma‘lum bir parametrlar yordamida aniqlanadi. Tasodifiylik darajasi yuqori psevdotasodifiy sonlar ketma-ketligini ishlab chiquvchi generatorlar zamonaviy kriptotizimlarning ajralmas qismi hisoblanadi, ushbu ketma-ketliklardan kriptografiyada quyidagi maqsadlarda foydalaniladi [2]:

– simmetrik kriptotizimlar uchun seans kalitlari va boshqa kalitlarni generatsiya qilishda;
– asimmetrik kriptotizimlarda qo‘llaniladigan yetarlicha katta uzunlikdagi matematik kattaliklar uchun boshlang‘ich tasodifiy qiymatlarni generatsiya qilishda (masalan katta tub sonlar generatsiyasi uchun);
– blokli shifrlash algoritmlarining SVS, OFB kabi tasodifiy boshlang‘ich qiymat talab qiluvchi rejimlari uchun tasodifiylik darajasi yuqori bo‘lgan vektorlar hosil qilishda;
– elektron raqamli imzo algoritmlarida foydalaniladigan katta uzunlikdagi parametrlar uchun tasodifiy qiymatlarni generatsiya qilishda;
– bir protokol orqali bir ma’lumotni har-xil jo‘natish uchun talab qilinadigan SSL va SET kabi protokollarda tasodifiy qiymatlarni hosil qilish va boshqalarda.

Ixtiyoriy ehtimollik taqsimoti qonuniyati bilan tasodifiy ketma-ketlik hosil qilish muammosi oxir-oqibatda tekis taqsimlangan ketma-ketlik generatsiyasi muammosiga keladi. Tekis taqsimlangan ketma-ketliklarda ixtiyoriy $t \in N$ tasodifiy qiymat uchun $x_t \in A$ ketma-ketlik to‘plamidagi elementning diskret tekis-taqsimlanganlik ehtimolligi $P\{x_t, A\} = 1/N$ ga tengdir [2]. Agar ushbu A ketma-ketlik to‘plamidagi har bir elementining ehtimolliklarining kvadratik farqlari 0,05 va 0,95 oraliqda yotsa bu ketma-ketlikni tasodifiy ketma-ketlik deb hisoblash mumkin.

Tekis taqsimlangan ketma-ketliklarning xossasiga ko‘ra, agar $A(a_i)$ - tekis taqsimlangan tasodifiy hamda $V(b_i)$ - tekis taqsimlangan va tasodifiy bo‘lmagan ketma-ketliklar bo‘lsa, u xolda $S(s_i) = A(a_i) \oplus V(b_i)$ - natijaviy ketma-ketlik tekis taqsimlangan tasodifiy ketma-ketlik bo‘ladi. Bu xossadan algoritmlarni kombinatsiyalashda foydalanish mumkin.

Tekis taqsimlangan tasodifiy ketma-ketliklar psevdotasodifiy ketma-ketliklar va haqiqiy tasodifiy ketma-ketliklarga bo‘linadi. Bunday ketma-ketliklarni quyidagi 2 xil usul bilan ishlab chiqish mumkin [1]:

– fizik generatorlar orqali;
– dasturiy generatorlar orqali.

Fizik generatorlar orqali ishlab chiqilgan ketma-ketlik haqiqiy tasodifiy ketma-ketlik hisoblanadi, bunday ketma-ketlik bir martagina ishlab chiqiladi va uni keyinchalik biror bir qonuniyat bilan huddi shunday ko‘rinishda generatsiya qilishning imkoniyati mavjud emas. Shu sababli fizik generatorlarda hosil qilingan kalitlarni oqimli shifrlashda qo‘llab bo‘lmaydi.

Dasturiy generatorlar yordamida hosil qilingan ketma-ketliklar psevdotasodifiy ketma-ketliklar deyiladi va bu ketma-ketliklarni generatsiya qilishda foydalanilgan kalitdan foydalanib xuddi shunday ko‘rinishda hamda yetarlicha uzunlikda qayta hosil qilish mumkin.

Oqimli shifrlash tizimlarida shifrlash va shifrni dastlabki matnga o‘girish jarayoni tez bo‘lishi uchun, faqat psevdotasodifiy hamda tekis taqsimlangan tasodifiy ketma-ketliklar hosil qiluvchi dasturiy generatorlardan foydalaniladi. Shu paytgacha ishlab chiqilgan tekis taqsimlangan ketma-ketliklarni hosil qiluvchi generatorlar va ular asosidagi oqimli shifrlash algoritmlari ma’lum bir yondashuvlar asosida yaratilgan.

Psevdotasodifiy ketma-ketliklarni hosil qiluvchi dasturiy generatorlarga asoslangan oqimli shifrlash algoritmlari asosan quyidagi yondashuvlar asosida yaratilgan [4,5]:

1. Tizimli-nazariy yondashuv asosida yaratilgan psevdotasodifiy generatorlar asosida ishlab chiqilgan algoritmlar;
2. Hisoblash murakkabligiga asoslangan yondashuv asosida yaratilgan psevdotasodifiy generatorlar asosida yaratilgan algoritmlar;
3. Kombinatsiyalashga asoslangan psevdotasodifiy generatorlar asosida yaratilgan algoritmlar.

Tizimli-nazariy yondashuv asosida oqimli shifrlash algoritmlarini yaratish ko‘p jihatdan blokli shifrlash algoritmlarini yaratishga o‘xshab ketadi. Mazkur yondashuv asosida yaratilgan oqimli shifrlash algoritmlarining kriptobardoshligi fundamental matematik me’zonlar va qonuniyatlar hisobga olingan holda murakkab bo‘lgan va yechish usuli noma’lum yoki mavjud emas deb hisoblangan muammoning qiyinchiligiga tenglashtiriladi. Matematikaning nazariy yutuqlari asosida yetarlicha katta davr uzunligiga ega, bloklari tekis taqsimlangan hamda chiziqsizlik kabi hususiyatlarga ega bo‘lgan ketma-ketlikllar hosil qiluvchi algoritmlar yaratiladi. So‘ngra yaratilgan algoritmni turli xil kriptotahlil usullariga bardoshliligi baholanadi. Agar yaratilgan algoritm mavjud kriptotahlil usullariga bardoshli bo‘lsa va hosil qilingan ketma-ketliklar tasodifiylik talablariga javob bersa, bu algoritmdan amaliyotda foydalanish mumkinligi to‘g‘risida ijobiy xulosa beriladi.

Dastlab yaratilgan oqimli shifrlash algoritmlari ham asosan tizimli–nazariy yondashuv asosida ishlab chiqilgan.

Tizimli-nazariy yondashuv asosida yaratiladigan oqimli shifrlash algoritmlariga quyidagi talablar mavjud [1,5]:

– algoritm asosidagi psevdotasodifiy ketma-ketlik generatori yetarlicha uzun davrga ega bo‘lgan ketma-ketliklar generatsiya qilishi;
– generatorning chiziqsiz murakkablik darajasi yuqori bo‘lishi;
– hosil qilingan psevdotasodifiy ketma-ketliklar bloklari tekis statistik taqsimot ko‘rsatkichiga ega bo‘lishi;
– psevdotasodifiy ketma-ketlikning gamma elementlari (bit, bayt, qism bloklari) boshqa barcha elementlarining ta’siri orqali hosil qilinishi, ya’ni samarali aralashish xususiyatiga ega bo‘lishi;

– psevdotasodifiy ketma-ketlikning gamma elementlarining keskin o‘zgarishi, ya’ni samarali tarqalish xususiyatiga ega bo‘lishi;

– algoritm akslantirishlarining bul funksiyalari chiziqsizlik shartini qanoatlantirishi hamda jadal samara (лавинный эффект) berishini ta’minlashi kerak.

Algoritmlarning ishonchliligini yoki bardoshliligini isbotlash qiyinligini tizimli-nazariy yondashuv asosida yaratilgan oqimli shifrlash algoritmlarining umumiy kamchiligi sifatida ko‘rsatishi mumkin.

Tizimli-nazariy yondashuv asosida yaratilgan oqimli shifrlash algoritmlari tarkibidagi generatorlarni yaratilish asoslariga ko‘ra elementar rekkurentlarga, siljitish registrlariga, bir tomonloma funksiyalarga, baytlar va bitlar bloklarining o‘rnini bog‘liqsiz almashtirishga asoslangan generatorlarga ajratish mumkin.

Hisoblash murakkabligiga asoslangan yondashuv matematikaning qiyin yechiladigan masalalariga asoslanadi. Hozirda matematikaning qiyin yechiladigan muammolari sifatida katta sonlarni tub ko‘paytuvchilarga ajratish, diskret logarifmlash, chekli maydonlarda yetarli darajada yuqori tartibli chiziqli tenglamalar sistemalarini yechish, elliptik egri chiziqlar bilan bog‘liq bo‘lgan murakkabliklarni yechish masalalarini ko‘rsatish mumkin. Aslini olganda, bu masalalarni nazariy jihatdan yechimlari topilgan va kompyuter tizimlari yordamida muvaffaqiyatli ravishda yechish mumkin. Lekin ma’lum bir katta parametrlar uchun tegishli masalaning yechilishi uchun talab qilinadigan resurslar (hisoblash va vaqt resursi) hozirgi kunda mavjud resurslar darajasidan oshib ketishi sababli yechilishi qiyin masalalar deb hisoblanadi [6].

Hisoblash murakkabligiga nazariy yondashuv asosida qurilgan oqimli shifrlash algoritmlarining amaliy bardoshliligi yuqorida keltirilgan matematikaning qiyin yechiladgan muammolari qiyinchiligiga tenglashtirish orqali isbotlanadi. Murakkablikka asoslangan algoritmlar tarkibidagi generatorlarni dasturiy yoki apparat-dasturiy jihatdan yaratish murakkabdir. Bunday oqimli shifrlash algoritmlarida juda katta sonlar ishlatilganligi, ko‘paytirish va darajaga oshirish kabi murakkab amallar qo‘llanilganligi sababli apparat va apparat dasturiy vositalarda amalga oshirish murakkablashib ketadi. Bu algoritmlarda shifrlash va shifrni ochish jarayoni sekin amaga oshirilganligi sababli tezlik va vaqtga sezgir (ovoz, video) axborotlarni uzatishda mazkur algoritmlardan foydalanib bo‘lmaydi. Bunday algoritmlardan maxfiylik darajasi yuqori bo‘lgan kichik hajmdagi axborotlarni, masalan, simmetrik blokli shifrlash algoritmlarining shifrlash kalitlarini uzatishda foydalanish maqsadga muvofiqdir.

Kombinatsiyalashgan nazariy yondashuv tizimli-nazariy va murakkablikka asoslangan yondashuvlar asosida ishlab chiqilgan algoritmlarni kombinatsiyalash asosida yangi algoritmlar yaratish usullari hisoblanadi.

Mazkur yondashuvda mavjud psevdotasodifiy ketma-ketliklar ishlab chiquvchi algoritmlarning (akslantirishlarning) kombinatsiyasi (birlashtirilishi) asosida yangi algoritm yaratiladi. Bu algoritmning bardoshliligi unda foydalanilgan tarkibidagi akslantirishlarning va algoritmlarning har birining murakkabligiga bog‘liq.

Kombinatsiyalash asosida psevdo-tasodifiy ketma-ketlik generatorlarini yaratish tasodifiy parametrli algoritmlarni kombinatsiyalash, polinomial kombi-natsiyalash, Maklaren-Marsali usullari orqali amalga oshiriladi.

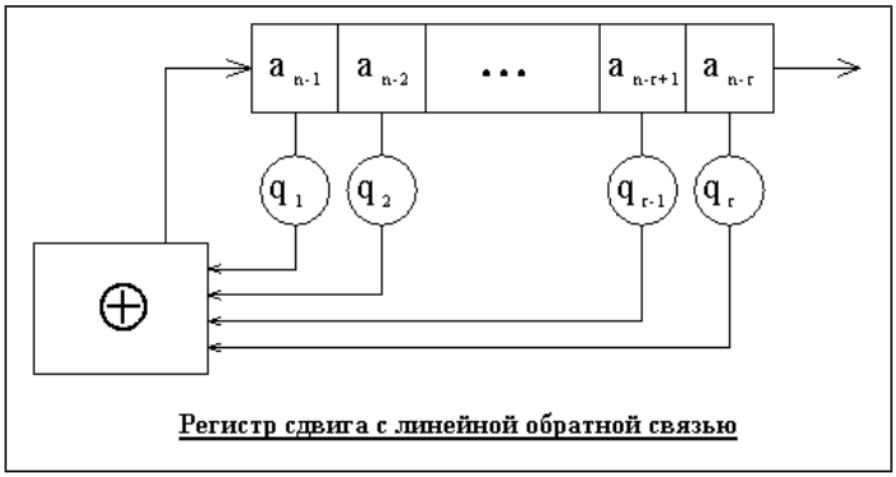
Hozirgi paytgacha foydalanib kelina-yotgan siljitish registrlariga asoslangan kriptobardoshli oqimli shifrlash algoritm-larining asosiy qismi siljitish registrlarini polinomial kombinatsiyalash usuli orqali yaratilgan.

Bugungi kunda keng foydalanib kelinayotgan oqimli shifrlash algoritm-larining ko‘pchiligining asosini siljitish registrlari, ya‘ni chiziqli teskari bog‘-lanishli siljitish registrlari tashkil qiladi. Ushbu siljitish registrlari Galua registrlari yoki Fibbonachi registrlari deb ham ataladi. Bu turdagi oqimli shifrlash algoritmlarining muvaffaqaiyatli qo‘l-lanilishiga quyidagilarni sabab sifatida ko‘rsatish mumkin [1,3].

1. Teskari bog‘lanishli siljitish registrlari asosida yaratilgan psevdotasodifiy sonlar generatorlari yordamida hosil qilingan ketma-ketliklarning statistik xarakteristikalari yaxshi hisoblanadi.

2. Bu turdagi generatorlarning xususiyatlarini tahlil qilish boshqa generatorlarga nisbatan oson hisoblanadi.

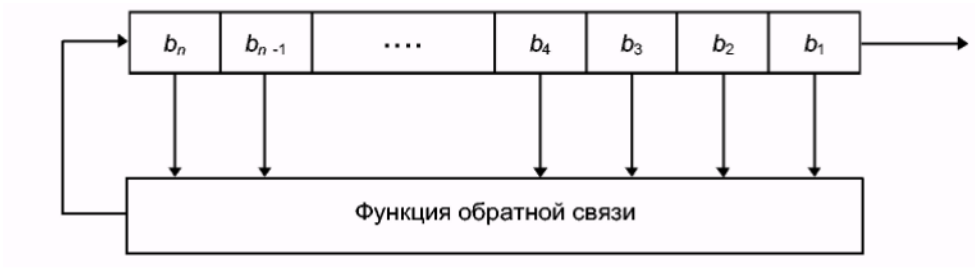
Teskari bog‘lanishli siljitish registrlari chiziqli teskari bog‘lanishli va chiziqsiz teskari bog‘lanishli siljitish registrlariga bo‘linadi. Siljitish registrlarining umumiy sxemasi 1-rasmda keltirilgan.



1-rasm. Teskari bog‘lanishli siljitish registrining umumiy ko‘rinishi

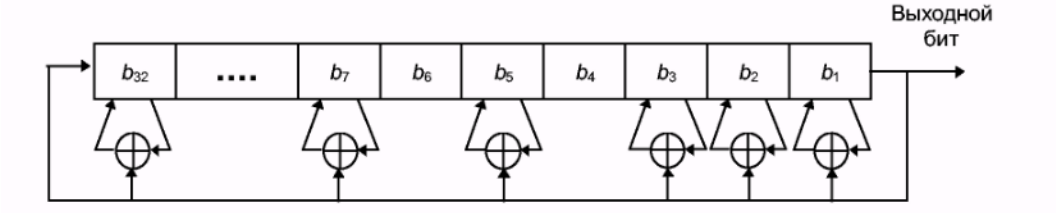
Siljitish registrlari asosida yaratilgan generatorlar siljitish registri va teskari bog‘lanish funksiyasidan iborat. Siljitish registrlariga asoslangan generatorlar asosida ishlab chiqilgan algoritmlarni dasturiy va apparat-dasturiy jihatdan amalga oshirish jarayonida, tez ishlashini ta’minlash uchun siljitish registri soni mikroprotsessorning registrlari soniga teng miqdorda tanlanadi. Hozirgi kunda mikroprotsserlarning asosiy qismi 64 razryadli registrlarda ishlaganligi sababli, dasturiy ta’minotda siljitish registrlari uzunligini 64 bitga teng qilib olish maqsadga muvofiq. Shunda to‘g‘ri tanlangan parametrlar asosida hosil qilingan ketma-ketlik davri maksimal, ya’ni 2^{64} bit ga yetishi ta’minlanadi. Siljitish registrlarining yana bir qismi teskari bog‘lanish funksiyasi hisoblanadi (2-rasm). Teskari bog‘lanish funksiyasi har bir taktda registrning ko‘phad bilan

ifodalanuvchi o‘rinlaridagi bitlar qiymatini XOR akslantirishi bilan qo‘shib, hosil bo‘lgan qiymatni registrning eng katta razryadi o‘rniga siljitish orqali kiritadi. Eng kichik razryad qiymati esa gammaga uzatiladi.

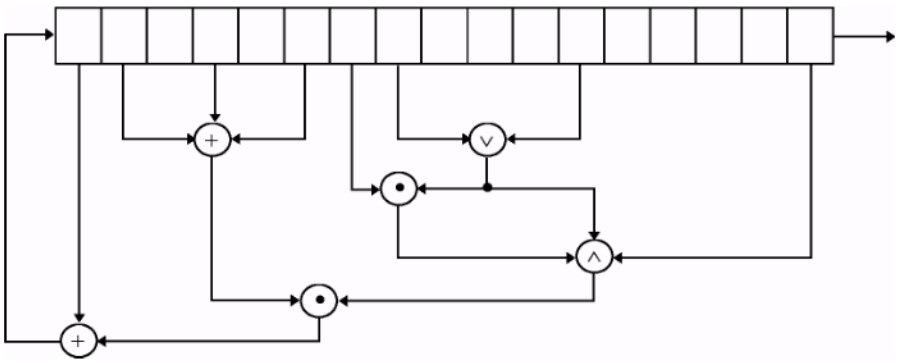


2-rasm. Chiziqli teskari bog‘lanishli siljitish registri

Chiziqli teskari bog‘lanishli siljitish registrlaridan biri Galua konfiguratsiyasidir (3-rasm). Galua konfiguratsiyasida gammaga uzatiladigan bit qiymati teskari bog‘lanish funksiyasida ishtirok etadi. Chiqish biti registrning har bir bitiga XOR amali orqali qo‘shiladi va registrning katta biti o‘rniga siljitish orqali beriladi. Eng kichik bit qiymati esa gammaga uzatiladi hamda teskari bog‘lanish funksiyasida ishlatiladi. Registrdan chiquvchi ketma-ketliklarining davri maksimal bo‘lishi uchun teskari bog‘lanish funksiyasi argumentlari registrning keltirilmaydigan ko‘phad hosil qiluvchi hadlaridan olinishi lozim.



3-rasm. Galua konfiguratsiyasiga asoslangan siljitish registri



4-rasm. Chiziqsiz teskari bog‘lanishli siljitish registri

Chiziqsiz teskari bog‘lanishli siljitish registrlarida teskari bog‘lanish funksiyasi bir necha xil chiziqsiz akslantirishlarni qo‘llash orqali amalga oshiriladi. 4-rasmda keltirilgan teskari bog‘lanish funksiyasida XOR, AND, OR mantiqiy

amallaridan foydalanilgan. Lekin, hozirgacha chiziqsiz siljitish registrlariga asoslangan generatorlar hosil qilgan ketma-ketliklarni yetarlicha tahlil qiluvchi matematik usullar ishlab chiqilmagan. Shu sababli chiziqsiz teskari bog‘lanishli registrlar orqali amalga oshirilgan generatorlarda quyidagi muammolarini ko‘rsatish mumkin:

– hosil qilingan psevdotasodifiy ketma-ketliklarda tekis taqsimot xarakteristikasidan chetlanish bo‘lishi mumkin, ya’ni “0” va “1” lar miqdori teng bo‘lmasligi mumkin;
– ketma-ketlikning davri kutilganidan qisqa bo‘lishi mumkin;
– boshlang‘ich qiymatlarning har xil qiymatlari uchun ketma-ketlikning davri har xil bo‘lishi mumkin, ya’ni ma’lum bir talabga javob beruvchi parametrlar tanlanganda har qanday ixtiyoriy boshlang‘ich qiymat uchun generator hosil qilgan ketma-ketlikning davri maksimal bo‘lmasligi mumkin;
– dastlab hosil qilingan ketma-ketlik tasodifiyga o‘xshab ko‘rinishi mumkin, lekin registrning ma’lum bir holati kelgandan keyingi hosil bo‘ladigan ketma-ketlik faqat “0” yoki “1” lardan iborat bo‘lib qolishi mumkin.

Blokli shifrlarga nisbatan solishtirganda uzluksiz shifrlarni ishlab chiqishning standart modeli mavjud emas, bu kriptograflarni bir qancha oqimli shifr modellarini ishlab chiqishga undaydi. Amalda foydalanish (tatbiq etish) maqsadlariga ko‘ra, oqimli shifrlar bir qancha toifalarga bo‘linadi va bu toifalar maxsus hossalarga ega bo‘lgan oqimli shifrlarni o‘z ichiga oladi. Mazkur toifalarni 3 ta asosiy yo‘nalishlari mavjud [7]:

– Apparat (Hardware) oqimli shifrlar;
– Dasturiy (Sofrware) oqimli shifrlar;
– Aralash (Gibrid) oqimli shifrlar.

Hardware asosidagi oqimli shifrlar klassifikatsiyasi o‘z ichiga FSSR/NLFR ga, soat nazoratiga va LFSR ga asoslangan oqimli shifrlarni oladi. Hardware oqimli shifrlarni qo‘llash ko‘pgina kriptografik dasturlarni himoyalashda muhim rol o‘ynaydi. DECIM v2, Edon-80, F-FCSR-H v2, Grain v1, MICKEY v2, MOUSTIQUE, POMARANCH v3, Tvirium kabi zamonaviy algoritmlar Hardware yo‘nalishida ishlab chiqilgan algoritmlar toifasiga misol bo’ladi.

Software asosidagi oqimli shifrlar T-funksiya, blokli shifr, S-blok hamda oddiy mantiqiy va arifmetik amallarni o‘z ichiga oladi. Mazkur toifadagi shifrlarni hardware asosidagi oqimli shifrlar bilan solishtirganda bitlar manipulyatsiyasiga (almashtirish, o‘rniga qo‘yish) asoslanganligi va mantiqiy ko‘rinishi bilan farqlanadi. Software aosidagi oqimli shifrlarga CryptMT v3, DRAGON, HC-128, LEX v2, NLS v2, Rabbit, Salsa20, SOSEMANUK kabi zamonaviy algoritmlarni misol sifatida keltirish mumkin.

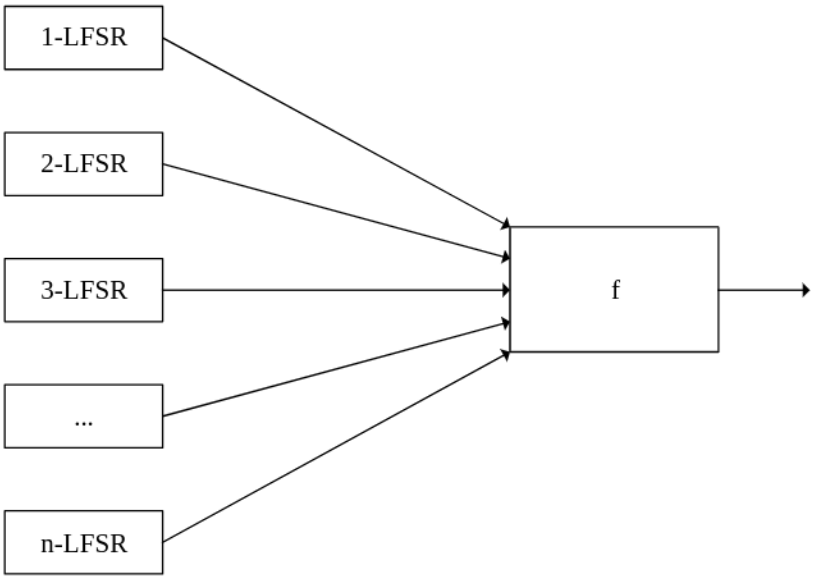
Gibrid asosidagi oqimli shifrlar hardware va software kombinatsiyasi asosida yaratilgan oqimli shifrlardan tashkil topadi. Mazkur toifadagi oqimli shifrlarning asosiy qismi LFSR ga asoslangan.

Generator funksiyalari berilgan dastlabki qiymatlar ustida ma’lum bir akslantirishlarni bajarish orqali sonlar ketma-ketligini hosil qilishga xizmat qiladi. Generator funksiyalarining quyidagi turlari mavjud:

– kombinatsion generatorlar;
– filtrlovchi generatorlar;
– vaqt nazorati generatorlari.

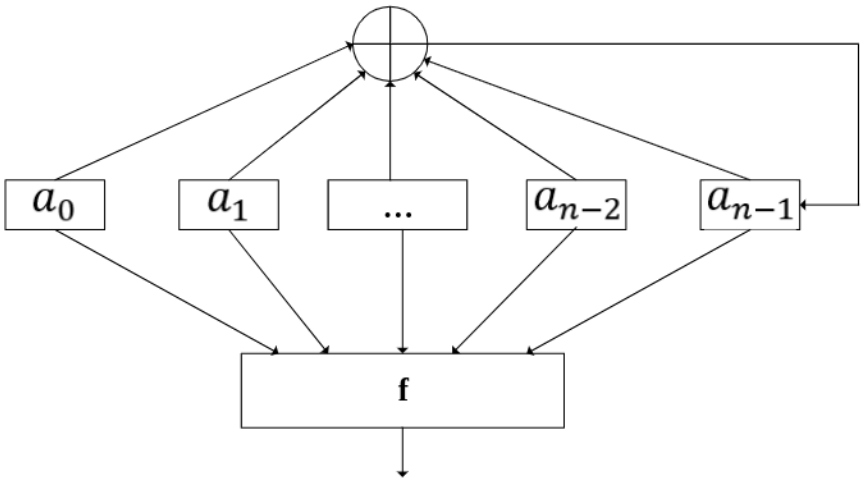
Kombinatsion generatorlar bir nechta teskari bog‘lanishli siljitish registrlarini birlashtirish (kombinatsiya qilish) orqali

quriladi (5-rasm, bu yerda: f – kombinatsiyalash funksiyasi).



5-rasm. Kombinatsion generatorlar

Filtrlovchi generatorlarda esa, yagona teskari bog‘lanishli siljitish registridan foydalaniladi (6-rasm, bu yerda: f – filtrlash funksiyasi).



6-rasm. Filtrlovchi generator

Vaqt nazorati generatorlarida ham kombinatsion generatorlaridagi kabi bir nechta teskari bog‘lanishli siljitish registrlaridan foydalanadi, faqat bunda registrlarning qiymatlari o‘zaro bir biriga bog‘liq bo‘ladi.

III. XULOSA

Oqimli shifrlash algoritmlari tahlili bo‘yicha, bloklab shifrlash algoritmlaridan farqli ravishda mazkur sohada kriptobardoshli uzluksiz shifrlash algoritmlarini yaratishning ko‘plab usul va yo‘nalishlar ishlab chiqilgan bo‘lishiga qaramasdan, ularning bir - biri bilan umumiyligini ifodalovchi yagona usullari mavjud emas [2].

Psevdotasodifiy sonlar ketma-ketligini ishlab chiquvchi generatorlar uzluksiz shifrlash tizimlarining ajralmas qismi hisoblanadi va bu tizimning bardoshliligi

mazkur generatorlarning bardoshliligiga bog‘liqdir. Oqimli shifrlash algoritmlarining bardoshligi bir alfavitli o‘rin almashtirish algoritmlari va bir martalik bloknot algoritmi bardoshliliklari oralig‘ida yotadi.

Psevdotasodifiy sonlar ketma-ketligini ishlab chiquvchi generator hosil qilgan ketma-ketliklar ko‘rinishidan haqiqiy tasodifiy ketma-ketlikka o‘xshaydi, lekin ushbu ketma-ketlikni aynan shunday generator va unda foydalanilgan kalit yordamida qayta hosil qilish mumkin. Bu xususiyat oqimli shifrlash algoritmlarining amaliyotda samarali qo‘llanilishini ta’minlaydi va kriptotizimning bardoshliligi darajasini bir martalik bloknot yordamida shifrlash algoritmi bardoshligigacha yetkazish imkonini beradi.

Keyingi tadqiqotlarda oqimli shifrlash algortimlarini baholashda qo‘llaniladigan kriptotahlil usullarini ko’rib chiqish maqsad qilingan.

Xulosa qilib aytadigan bo‘lsak ushbu maqolada kvant algoritmlarni yechishda qo‘llaniladigan qcl (quantum computation language) tili, uning operatorarining ishlash jarayonlari va Deutsch algorimini ishlash prinsiplari keltirib o‘tilgan. Kvant jarayonlarning asosiy tamoyillari, fizikaviy va algoritmik talqinlari hisobga olingan. Ushbu jarayonlar tizimni tahlil qilishda global optimallash muammolariga samarali yechimlarni qidirishda va kutilmagan holatlarni oqilona boshqarishda qo‘llaniladigan algoritmning tasniflari keltirilib o‘tilgan.

Hozirgi vaqtda kalitlarni taqsimlash muammosida kvant kriptografiyasi assimetrik shifrlash tizimlariga yagona muqobildir. Yuqoridagilarni hisobga olgan holda, assimetrik shifrlash tizimlarini buzish murakkabligi sezilarli darajada pasaygan taqdirda, kvant kriptografiyasi rivojlanish uchun potensialga ega.

Biroq, kvant kriptografiyasining tamoyillari va usullaridan foydalangan holda tizimlarni tashkil qilishning yuqori texnologik murakkabligi, hatto zamonaviy texnologiyalarning etarlicha yuqori darajada rivojlanishi bilan ham assimetrik tizimlarni siqib chiqarishga imkon bermaydi.

ADABIYOTLAR

[1] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М., Изд. ТРИУМФ, 2003. – 816.
[2] *Харин Ю.С, Берник В.И, Матвеев Г.В, Агиевич С.В.* Математические и компьютерные основы криптологии: Учебное пособие. – Минск, ООО «Новое знание», 2003. – 382.
[3] *Асосков А.В, Иванов М.А.* Поточные шифры, М: Кудиц-Образ, 2003. – 336.
[4] *Akbarov D.Ye.* Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi. – Toshkent, «O‘zbekiston markasi» nashriyoti, 2009. – 432.
[5] http://www.cryptography.ru
[6] *Musayev A.I.* Mavjud oqimli shifrlash algoritmlari asoslarini tadqiq qilish va yangi kriptobardoshli algoritmlar yaratish. Axborot xavfsizligi yo‘nalishi bo‘yicha magistr darajasidagi dissertatsiya ishi. Toshkent, 2008.
[7] *Suwais K., Samsudin A.* New Classification of Existing Stream Ciphers. Universiti Sains Malaysia (USM), Malaysia 2010.

Поступила в редакцию 9.11.2022

Citation: *Rahmatullayev I.R.* (2022). Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 2(2). – B. 119-128.

STREAM ENCRYPTION ALGORITHMS AND THE BASIS OF THEIR CREATION

Rahmatullaev I.R.[1]

[1] Samarkand branch of Tashkent University of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan

ilhom9001@gmail.com

Abstract. *This article analyzes stream encryption algorithms belonging to the family of symmetric encryption algorithms and their creation bases, as well as types of pseudo-random number generators and development bases. Pseudo-random generators based on the system-theoretical approach, pseudo-random generators based on the approach based on computational complexity and combinations, and stream encryption algorithms based on them are reviewed.*

Keywords: *Stream ciphers, XOR, SVS, OFB, SSL, SET, LFSR, Hardware, Software, Hybrid, combinational generators, filter generators, time control generators.*

АЛГОРИТМЫ ПОТОКОВОГО ШИФРОВАНИЯ И ПРИЧИНЫ ИХ ПОЯВЛЕНИЯ

Рахматуллаев И.Р.[1]

[1]Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан

ilhom9001@gmail.com

Аннотация. *В данной статье рассматривается параметры безопасности с помощью алгоритма потокового шифрования, также рассматривается метод генерации псевдочисел на наличии обработки потоковых данных. Системный анализ псевдогенерирующих чисел, рассмотрения, комбинированного подходов данных с алгоритмом потокового шифрования*

Ключевые слова: *потоковое шифрование, XOR, SVS, OFB, SSL, SET, LFSR, Hardware, Software, Gidrid, комбинационное шифрования, генератор фильтров, генератор включающий время.*