OQIMLI SHIFRLARNING QURILISH PRINSIPLARI

Mamarajabov Husan Ergash o‘g‘li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: husankarimov09@gmail.com
Tel: +998945169616
Shukurov Dadanur Tohir o`g`li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: dadanur0094@gmail.com
Tel: +9989977420094
Xurramov Azizjon Baxodir o`g`li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: azizbekxurramov0102@gmail.com
Tel: +998907472494

Annotatsiya: Blok algoritmi ma'lum uzunlikdagi bloklarni shifrlash uchun mo‘ljallangan. Biroq, ma'lumotlarni bloklarda emas, balki, masalan, belgilar bo‘yicha shifrlash kerak bo‘lishi mumkin. Oqimli shifrlash kiruvchi xabarni har bir operatsiya uchun bir bit (yoki bayt)ga aylantiradi. Oqimli shifrlash algoritmi xabarlarni etarlicha katta uzunlikdagi bloklarning butun soniga ketma-ket bo‘lish zaruratini yo‘q qiladi va real vaqtda ishlay olmaydi. Shunday qilib, agar belgilar oqimi uzatilsa, har bir belgi shifrlanishi va bir vaqtning o‘zida uzatilishi mumkin.

Kalit so‘zlar: Oqimli shifrlash, shifr matn, kalit bitlari, Vernam shifri, oqimli kriptotizimlar, sinxron, assinxron.

Ochiq matn belgisining ochiq matnda joylashuvi va foydalanaladigan kalitga bog‘liq holda har belgini shifr matn belgisiga almashtiradigan simmetrik shifr oqimli shifr deyiladi. Belgi sifatida alohida bitlar hamda alohida belgilar ishtirok etishi mumkin[1]. Oqimli shifrlar bilan tovush, video kabi ma’lumotlarning uzluksiz oqimini shifrlash qulay.

Oqimli shifrlarda har bir amal natijasida ochiq matnning bitta biti (yoki belgisi) ni shifr matnning bitta biti (yoki belgisi) ga almashtiradi. Kalit oqimi generatori k_1, k_2, ..., k_i bitlar oqimini generatsiya qiladi. Ushbu bitlar oqimi va ochiq matn bitlari oqimi p_1, p_2, ... , p_i, ... , p_z ni ikkining moduli bo‘yicha qo‘shish natijasida shifr matn bitlari oqimi hosil bo‘ladi:

$c_i = p_i \oplus k_i$.

Dastlabki matnga o‘girishda shifr matn va kalit bitlari oqimlari ustida XOR amali bajariladi:

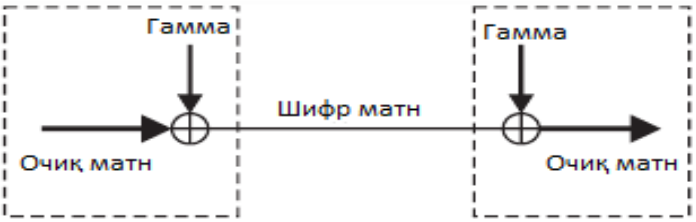
$p_i = c_i \oplus k_i$.

Ko‘rinib turibdiki, $k_i = p_i \oplus c_i$ o‘rinli.

Shunday qilib, oqimli shifrlashda belgilar bo‘yicha shifrlash kriptotizim ishini kechiktirmaydi, aksincha, shifrlashni yuqori tezlikda, kiruvchi axborotni kirish tezligida amalga oshishini ta’minlaydi. Bu esa o‘z navbatida axborot va ma’lumotlar oqimi razryadi hajmi qanaqa bo‘lishidan qat’iy nazar shifrlashni real vaqtda amalga oshirishga xizmat qiladi.

Oqimli shifrga klassik misol sifatida Vernam shifri yoki bir martalik bloknot deb nomlanuvchi shifrni ko‘rsatish mumkin. Agar gamma sifatida tasodifiy bitlar ketma-ketligidan foydalanilsa hamda gammaning uzunligi hech bo‘lmaganda xabarning uzunligiga teng bo‘lsa, u holda Vernam shifrini amalda buzish mumkin emas. Ushbu shifrning kamchiligi xabarning uzunligidan kam bo‘lmagan uzunlikdagi kalitni saqlash va qabul qiluvchiga yetkazishdan iborat. Bu esa amalda murakkab masala hisoblanadi. Shu sababli zamonaviy oqimli shifrlarning asosiy g‘oyasi gamma uchun psevdotasodifiy sonlar ketma-ketligini generatsiya qilish imkonini beruvchi, kichik uzunlikdagi maxfiy kalitdan foydalanib, bir martalik bloknot konsepsiyasini amalga oshirishdan iborat.

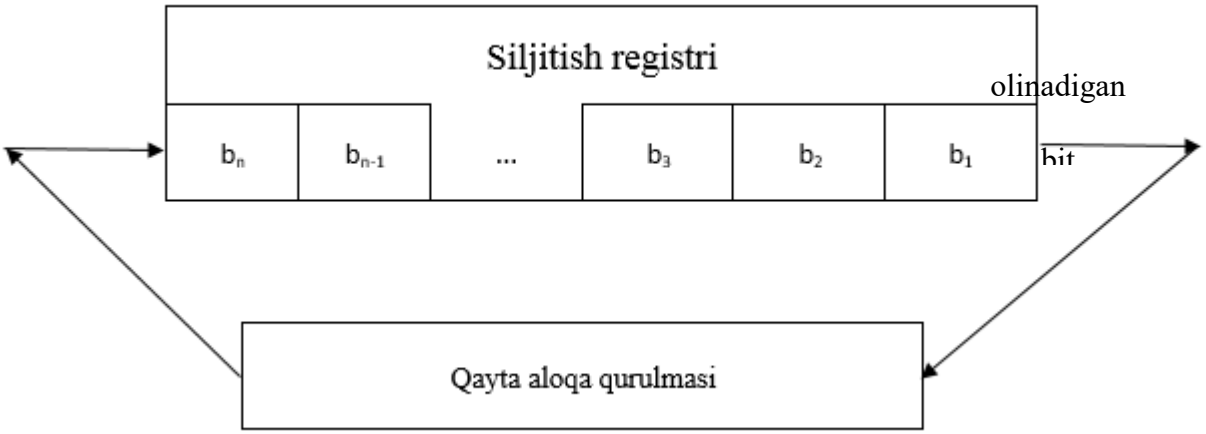
Oqimli shifrni umumiy sxemasi quyidagicha tasvirlanishi mumkin (1- rasm).



2-rasm. Oqimli shifr sxemasi.

Faraz qilaylik, oqimli shifrlashning gammalashtirish jarayonida aloqa kanalidan uzatishda shifrmatnning bitta belgisi o‘zgarib ketdi. Ushbu holda dastlabki matnga o‘girish jarayonida shifr matnning ushbu belgisidan boshqa barcha belgilari, ya’ni o‘zgarmagan belgilari ochiq matn belgisi sifatida to‘g‘ri o‘giriladi[3].

Agar aloqa kanalidan uzatishda shifr matndagi bitta belgi tushib qolsa, u holda shifr matnning ushbu belgidan keyin keluvchi barcha belgilari noto‘g‘ri o‘giriladi. Ma’lumotlarni uzatish kanallarining deyarli barchasida oqimli shifrlash tizimlari uchun shovqin mavjud bo‘ladi. SHu bois, axborotni yo‘qolishini bartaraf qilish maqsadida matnlarni shifrlash va dastlabki matnga o‘girish jarayonlarini sinxronlantirish muammosini hal qilish lozim bo‘ladi. Ushbu muammoni hal qilish usuliga ko‘ra oqimli kriptotizimlar sinxron va asinxron (o‘z-o‘zidan sinxronlanuvchi) turlarga bo‘linadi. Psevdo-tasodifiy oqimni olish uchun qayta aloqa bilan siljish registrlaridan foydalanish mumkin. Teskari aloqani almashtirish registri ikki qismdan iborat: haqiqiy n-bitli siljish registri va qayta aloqa qurilmasi.

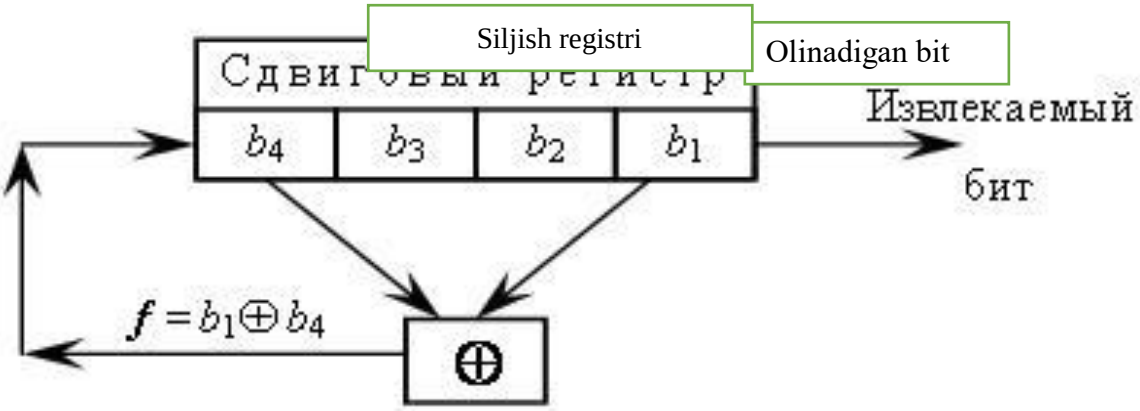


2-rasm. Siljitish registirining umumiy ko‘rinishi.

Shifr registridan bir vaqtning o‘zida faqat bitlarni ajratib olishingiz mumkin. Quyidagilarni chiqarib olishingiz kerak bo‘lsa , barcha bitlar registrlar o‘ngga 1 bitga siljiydi. Bunday holda, chapdagi registrning kiritilishi yangisini oladi, bu qayta aloqa qurilmasi tomonidan ishlab chiqariladi va siljish registrining barcha boshqa bitlariga bog‘liq. Shu sababli, registr bitlari ma’lum bir qonunga muvofiq o‘zgaradi, bu PRNGni olish sxemasini belgilaydi. Ko‘rinib turibdiki, registrning ma’lum miqdordagi davrlaridan keyin bitlar ketma-ketligi takrorlana boshlaydi. Olingan ketma-ketlikning takrorlanish boshlanishidan oldingi uzunligi siljish registrining davri deb ataladi. O‘zgartirish registrlari yordamida oqim shifrlari amaliyotda uzoq vaqt davomida qo‘llanilgan. Bu ularning raqamli uskunalar yordamida juda yaxshi amalga oshirilganligi bilan bog‘liq.

Teskari aloqani o‘zgartirish registrining eng oddiy turi bu chiziqli fikr almashish registridir (chiziqli fikr-mulohaza siljish registrlari–LFSR).Ushbu qurilmadagi fikr-mulohazalar oddiygina registrning barcha (yoki ba’zi) bitlarining modul 2 yig‘indisi sifatida amalga oshiriladi. Teskari aloqada ishtirok etuvchi bitlar teginish ketma-ketligini hosil qiladi. Chiziqli qayta aloqa o‘zgarishi registrlari yoki ularning modifikatsiyalari ko‘pincha kriptografiyada qo‘llaniladi.

Bu qanday ishlashini tushunish uchun fikr almashish registri , 4-bitni ko‘rib chiqing. Birinchi va to‘rtinchi raqamlardan teginish bilan LFSR , rasmda ko‘rsatilgan



3-rasm.

Har bir qadamda registrning butun tarkibi bir bitga o‘ngga siljiydi. Bunday holda, natijada bittasini olish mumkin. Bo‘sh chap tomonda joy keladi geribildirim funksiyasini baholash natijasiga teng bit f = b_1 □ b_4. Psevdo-tasodifiy generatorning chiqish ketma-ketligi jadvalning oxirgi ustunini tashkil qiladi (qayta olish mumkin). Chiziqli siljish registrining kattaligi n bit 2 dan birida bo‘lishi mumkin n-1 holatlar (faqat nollar registrining holati bundan mustasno - bunday holat paydo bo‘lganda, faqat nollar hosil bo‘ladi va yaratilgan ketma-ketlikning psevdo-tasodifiyligi haqida gapirishning hojati yo‘q). Shuning uchun, nazariy jihatdan registr maksimal 2 davri bilan psevdo-tasodifiy ketma-ketlikni yaratishi mumkin. Chiziqli fikr almashish registri faqat aniq bo‘lganda maksimal davrga ega bo‘lgan t siklik bit ketma-ketligini hosil qiladi. Raqamlarning tegishli raqamlarini tanlash imkonini beruvchi matematik nazariya ishlab chiqildi. Teskari aloqa bilan chiziqli siljish registrlari ko‘pincha ishlatilgan va ma’lumotlar oqimini shifrlashda hozir ham qo‘llaniladi. Bunday shifrlash qurilmalarida kriptografik kuchni oshirish uchun bir nechta siljish registrlarining qayta aloqa bilan kombinatsiyasi va qo‘shimcha aralashtirish qo‘llaniladi. Bunday elektron sxemalar ikkinchi jahon urushidan oldin ham taklif qilingan va ishlab chiqarilgan. Shunga o‘xshash printsiplar ba’zilarida o‘rnatilgan 20-asr oxirida yaratilgan oqim shifrlari, masalan, A5 algoritmi yevropada standartning uyali raqamli aloqa kanallarini shifrlash uchun ishlatiladi. Ba’zi kriptoanalitiklar chiziqli qayta aloqa almashinuvi registrlari yordamida oqimlarni shifrlash algoritmlarining ishonchliligiga shubha bildirgan bo‘lsa-da, ular hozirgi kunga qadar qo‘llanilgan turli xil harbiy va fuqarolik aloqa qurilmalarining ishlashi uchun asosdir.

Chiziqli siljish registrlari asosidagi psevdo-tasodifiy sonlar generatorlarining asosiy kamchiligi dasturiy ta’minotni amalga oshirishning murakkabligi hisoblanadi. Shiftlar operatsiyalari elektron qurilmalarda oson va tez amalga oshiriladi, shuning uchun turli mamlakatlarda qayta aloqa almashinuvi registrlari yordamida algoritmlarga asoslangan oqim shifrlash uchun mikrosxemalar va qurilmalar ishlab chiqariladi.

Psevdo-tasodifiy raqamlarni olish uchun blokli shifrlarning OFB va CTR rejimlaridan foydalanish:

Siz har qanday blokli shifrlash algoritmlaridan foydalanishingiz mumkin, masalan AES yoki GOST 28147-89, blokli shifrlarning OFB va CTR rejimlaridan foydalangan holda ma’lumotlarni oqimli shifrlash uchun. OFB rejimi nomi (Chiqish Feedback) deb tarjima qilinadi.

Xulosa. Oqimli shifrlashda bajaradigan shifri kirish xabarini har bir operatsiya uchun bir bit (yoki bayt) shifrlash . mos ravishda shifrlash algoritmi xabarni bo‘lish zaruratini yo‘q qiladi. Shunday qilib, agar uzatilsa belgilar oqimi, har bir belgi bir vaqtning o‘zida shifrlanishi va uzatilishi mumkin. Oqim shifrlari real vaqtda ma‘lumotlarni shifrlash uchun ishlatiladi. Oqim shifrlarida kalit generatorlar sifatida foydalanish mumkin psevdo-tasodifiy raqamlar generatorlari (PRNG). PRNG dan foydalanishdan maqsad kalitning o‘zi nisbatan kichik uzunlikka ega bo‘lgan “cheksiz” kalit so‘zni olishdir.

Foydalanilgan adabiyotlar:

1. Akbarov D. E. “Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi” – Toshkent, 2008

2. Matt J. B. Robshaw, Current Ciphers TR-701 Technical Report, Version 2.0, RSA Laboratories, 1995 year

3. Bet, Tomas; Piper, Fred (1985). Stop and Go Generator.