ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ә. Бүркітбаев атындағы өнеркәсіптік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыш технологиялар кафедрасы

Мендияров Жігер Ерікұлы

Телекоммуникациялық жүйелерде ақпаратты криптографиялық қорғаудың симметриялық алгоритмдерін құру

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ә. Бүркітбаев атындағы өнеркәсіптік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыш технологиялар кафедрасы

5В071900 – Радиотехника, электроника және телекоммуникация

ҚОРҒАУҒА ЖІБЕРІЛДІ
ЭТ ж ҒТ кафедра меңгерушісі
_____И. Сыргабаев
«_____» _____2020ж.

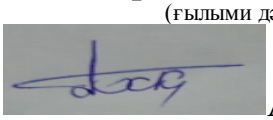
Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы Телекоммуникациялық жүйелерде ақпаратты криптографиялық қорғаудың симметриялық алгоритмдерін құру

5В071900 – Радиотехника, электроника және телекоммуникация мамандығы

Орындаған: Ж.Е. Мендияров

Рецензия беруші
ҚазҰАУ. доктор PhD, қаум-н проф
(ғылыми дәрежесі, атағы)
_____Н.Б. Әлібек
«25» мамыр 2020ж .

Ғылыми жетекші
РЭжТкаф. PhD док-р., сен-р лектор
(ғылыми дәрежесі, атағы)
 А. Хабай
«18» мамыр 2020ж.

Алматы 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ә. Бүркітбаев атындағы өнеркәсіптік автоматтандыру және цифрландыру институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

5В071900 – Радиотехника, электроника және телекоммуникация

БЕКІТЕМІН
ЭТ ж ҒТ кафедра меңгерушісі
_____И.Сыргабаев
«21» қараша 2020ж.

Дипломдық жоба орындауға
ТАПСЫРМА

Білім алушы *Мендияров Жігер Ерікұлы*
Тақырыбы: *Телекоммуникациялық жүйелерде ақпаратты криптографиялық қорғаудың симметриялық алгоритмдерін құру.*
Университет ректорының *“27”қаңтар 2020ж. №726-б бұйрығымен бекітілген*
Аяқталған жобаны тапсыру мерзімі *“02” маусым 2020ж*
Дипломдық жобаның бастапқы берілістері; Дипломдық жұмыста криптографиялық алгоритмдердің тұрлері мен негізгі әдістеріне қысқаша шолу жасалды. Сонымен қатар телекомуникаця жүйесінде GSM ұялы стандартына криптографиялық алгоритмдерін енгізу бағытарына талдаулар жасалды. СКБЖР негізінде құрылған криптографиялық алгоритмды ұялы байланыс жүйесінде қолдану технологиясына талдау жасап, криптотөзімділікті арттыру мақсатында ауыспалы «тоқта-кетті» генераторына әртүрлі ұзындықтағы үш жылжу регистрін қолдануды қарастру.
Дипломдық жобада қарастырылатын мәселелер тізімі:
а) Т*елекомуникация жүйесіндегі ақпаратты криптографиялық қорғаудың алгоритмдері.*
ә) 2 Ұялы байланыс жүйесіне қолданылатын криптологиялық шифрлау технологясын
б) Сызықтық кері байланысы бар жылжу регистрі құрылымы талдау.
в) берілген ақпаратты қорғаудың жаңа симметриялық кілт шифрлау алгоритмін құру.
г) Құрылған шифрлық тізбектің криптографиялық тұрақтылығын арттыру жолдары.
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс) *Сызықтық кері байланысы бар жылжу регистрі және СКБЖР көмегімен*

деректерді шифрлау схемасы, Сызықты кері байланысы бар жылжу регистрі тіркеу жұмысы, MATLAB - SIMULINK қолдана отырып (1+x3+x5) көпмәнді 5 биттік СКБЖР енгізу, SIMULINK- MATLAB ортасындағы криптографиялық шифрлау алгоритім моделі .

Ұсынылған негізгі әдебиет *Bruce Schneier, "Applied Cryptography," John Wiley & Sons Inc., 1996, New York[2] Raj Pandya, "Mobile and Personal Communication Systems and Service"s, 2001 IEEE PRESS, New York. V. K. Garg, "Wireless and Personal Communication System", 1997, Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. – К.: МК-Пресс, 2005. – 288 с.*

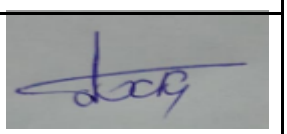
дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Телекоммуникация жүйелерідегі ақпартты тарату қауіпсіздігін қамтамасыз етудің негізгі мақсаттары, әдістері.	13.01.2020	Орындалды
Matlab програмасы көмегімен дыбыстық сигналды сандық сигналға түрлендіу. Сандық аудио сигналды виртуалды схемамен шифрлау.	10.02.2020	Орындалды
Берілген ақпаратты қорғаудың жаңа симметриялық кілт шифрлау алгоритмін құру	20.04.2020	Орындалды

Дипломдық жұмыс бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	А.Хабай PhD доктор., сенер лектор	18.05.2020ж	

Ғылыми жетекшісі  Хабай Анар

Тапсырманы орындауға алған білім алушы  Ж.Е.Мендияров

Күні "21" қараша 2020 ж.

АҢДАТПА

Дипломдық жұмыста криптографиялық алгоритмдердің тұрлері мен негізгі әдістеріне қысқаша шолу жасалды. Сонымен қатар телекомуникаця жүйесінде GSM ұялы стандартына криптографиялық алгоритмдерін енгізу бағытарына талдаулар жасалды. Сызықтық кері байланысы бар жылжу регистрының негізінде құрылған криптографиялық алгоритмды ұялы байланыс жүйесінде қолдану технологиясына талдау. Криптотөзімділікті арттыру мақсатында ауыспалы «тоқта-кетті» генераторына әртүрлі ұзындықтағы үш жылжу регистрін қолдануды қарастрылды.

Ұялы байланыс жүйесіне сызықтық кері байланысы бар жылжу регистры негізінде құрылған криптографиялық алгоритмды MATLAB.SIMULINK-ортасында моделденді.

АННОТАЦИЯ

В дипломной работе был проведен краткий обзор основных методов и задач криптографических алгоритмов. Также был проведен анализ направлений внедрения криптографических алгоритмов в системе телекомуникации GSM. Анализ технологии использования криптографического алгоритма в системе сотовой связи, построенного на основе регистра движения с линейной обратной связью. В целях повышения криптостойкости предусматривается использование трех регистра сдвигов различной длины на переходный генератор «стоп-ушел».

Криптографический алгоритм на основе регистра сдвига с линейной обратной связью с системой мобильной связи был смоделирован в среде MATLAB.SIMULINK.

ANNOTATION

Diploma work provides a brief overview of the types and basic methods of cryptographic algorithms. In addition, the analysis of the implementation of cryptographic algorithms in the GSM mobile standard in the telecommunications system was analyzed. Analysis of the technology of application of cryptographic algorithms based on the *linear feedback shift register* in mobile communication systems. In order to increase the resistance of cryptography, it is planned to use three shift registers of different lengths in the variable " *Stop*-and-Go" generator.

The cryptographic algorithm created on the basis of linear feedback shift register for mobile communication systems was modelled in MATLAB.SIMULINK-environment.

МАЗМҰНЫ

КІРСПЕ

Телекомуникаця жүйесінде GSM ұялы стандартының криптографиялық алгоритмдерін енгізу қазыргі таңның маңызды мәселелерінің бірі. Ортақ тарату құралын пайдаланған кезде қандай да бір ақпарат қаупсіздігін қорғайтын әдіс орнатылмаса, онда жеке құпиялық сақталмауы мүмкін. Криптографиялық сақтық жеке меншік ақпаратының қауіпсіздігін бақылауды қалпына келтіруге мүмкіндік береді. GSM ұялы телефондарындағы сөйлесулердің құпиялығын қамтамасыз ету үшін қолданылатын A5/x шифрлау алгоритмдері әдістері бар[1].

Шифрлау алгоритмдері ақпараттың құпиялығын қамтамасыз ету мәселесін шешуге арналған. Қазіргі уақытта ақпаратты қаупсіздігін сақтау да криптографиялық әдістер қолданылады. Ежелгі заманнан бері шифрлау ең тиімді қорғаныс нысаны болып келеді және солай болып қала береді.

Шифрлау дегеніміз - қорғалмаған (ашық) ақпаратты шифрланған (жабық) пішінге шифрмәтінге[2], яғни шабуыл жасаушыға толық қол жетімді болмайтындай оны өзара өзгерту. Шифрлау кезінде кілттер қолданылады, олардың болуы ақпаратты шифрлау немесе дешифрлау мүмкіндігін білдіреді. Қазіргі криптожүйелерді құпия (симметриялы) кілтпен және ашық (асимметриялық) кілтпен криптожүйелерге қолданылады[3]. Егер шифрлау және шифрын ашу үшін бірдей кілт пайдаланылса, мұндай криптожүйе симметриялы деп аталады.

Бұл дипломдық жұмыста біз OFB (Output Feedback)[4] – шығу бойынша кері байланыс әдісін пайдалану арқылы ұялы байланыстағы ақпаратты шифрлау әдісі қарастрылады. **Сызықтық кері байланысы бар жылжу регистрының** СКБЖР негізінде құрылған криптографиялық алгоритмдердің жылдамдығы жоғары сондайақ барлық есептеуіш құрылғыларда аппараттық түрде іске асруға болатын қарапайым биттік операцияларды қосу және көбейту ғана қолдану; жақсы криптографиялық қасиеттері (СКБЖР жақсы статистикалық қасиеттері бар үлкен кезеңнің кезектілігін тудыруы мүмкін) өз құрылымының арқасында СКБЖР алгебралық әдістерді қолдана отырып оңай талданады.

1. Телекомуникация жүйесіндегі ақпаратты криптографиялық қорғаудың алгоритмдері

1.1 Симметриялы алгоритмды криптожүйелер

Шифрлау алгоритмдері ақпараттың құпиялығын қамтамасыз ету мәселесін шешуге арналған. Қазіргі уақытта ақпаратты жабу үшін криптографиялық әдістер қарқынды қолданылады. Ежелгі заманнан бері шифрлау ең тиімді қорғаныс нысаны болып келеді және солай болып қала береді. Осылайша, шифрлау тұрақты болуы тиіс, егер криптоаналитикада қолданылатын кілттің мәні шифрлеудің барлық алгоритмі белгілі болса да ол ақпарат қаупсіздігін қорғайалатын шифрлық бағдарламаның толық мәтініне ие болуы керек. Тәжірибе көрсеткендей, шифрлау алгоритм неғұрлым көп болған сайын, адамдар онымен көбірек жұмыс істеді, соғұрлым дәлелдеулер болады, сондықтан ол сенімді. Осылайша, көпшілікке белгілі алгоритмдер уақыттың күресіне төтеп береді, бірақ құпия шифрларлау барсы көптеген қателіктер мен кемшіліктерді көрсетті, өйткені бәрін ескеру мүмкін емес[5].

Шифрлау алгоритмі, егер жабық деректер болса және құпия кілт білсе, ашық деректер туралы ақпарат алу мүмкін болмаса, тұрақты болып саналады. Құпия кілттің өлшемі шифрланатын деректердің мөлшеріне тең (немесе одан көп) жағдайды қоспағанда, мүлдем тұрақты Шифр құрудың мүмкін еместігі қатаң дәлелденген. Бұл жағдайды іс жүзінде жүзеге асыру қиын, өйткені. ол үшін жабық мәтін бойынша ашық мәтінді қалпына келтіру міндеті қиын есептелінетін шифрларды пайдаланады, яғни шабуыл экономикалық мақсатқа сай емес болып, соншалықты үлкен ресурстарды талап етеді[6].

1.1.2 Симметриялық криптожүйелерді құрудың жалпы әдістері

Гамма-шифр – ашық деректерді шифрлау және шифрланған мәліметтерді шифрлау үшін берілген алгоритм бойынша жасалған жалған кездейсоқ тізбек[7].

Гаммалау – бұл белгілі бір заңға сәйкес шифрдің гамма-нұсқасын ашық деректерге қолдану процесі.

Шифрлау алдында ашық деректер ұзындығы бірдей T_0^i блоктарына бөлінеді (әдетте 64, 128, 196 немесе 256 бит). Шифр гаммасы ұқсас ұзындықтағы G_c^i блоктарының жүйелілігі түрінде шығарылады:

$$T_c^i = G_c^i \oplus T_0^i,\ i = \overline{1, m,} \tag{1.1}$$

мұндағы m – ашық мәтін блоктарының саны.

Шифрлау процесі гамманы қайта генерациялауға және шифрланған деректерге осы гамманы салуға әкеледі:

$$T_0^i = G_c^i \oplus T_c^i,\ i = \overline{1, m.} \quad (1.2)$$

Шифрлардың тұрақтылығы кілттің ұзындығымен анықталады.

Жалған кездейсоқ тізбектерді генерациялау үшін криптографиялық тұрақты генераторлар қолданылады. Оларға мынадай талаптар қойылады:

- гамма кезеңі өте үлкен болуы керек;
- гамма алдын-ала болжанбауы керек;
- гамма жасау үлкен техникалық қиындықтар туғызбауы керек.

Шеннонның пікірі бойынша практикалық шифрларда екі жалпы қағидатты (принципті) қолдану қажет – тарату және араластыру.

Тарату – жай мәтіннің статистикалық қасиеттерін жасыруға мүмкіндік беретін қарапайым мәтіннің бір таңбасының шифрмәтіннің көптеген белгілеріне әсерінің таралуы.

Араластыру – ашық және шифрланған мәтіндердің статистикалық қасиеттерінің өзара байланысын қалпына келтіруді қиындататын шифрлаушы түрлендірулерді қолдану.

Қазіргі заманғы симметриялы криптожүйелер – бұл қарапайым шифрлардың кейбір бірізділігі түрінде іске асырылған құрамдас шифрлар, олардың әрқайсысы жиынтық таратуға және араластыруға өз үлесін қосады. Қарапайым шифрлар ретінде жиі ауыстыру (замены) және алмастыру (перестановки) шифрларын қолданады. Қазіргі заманғы блоктық шифрда блоктар ұзындығы 64,128,192 немесе 256 бит екілік тізбектер болып табылады. Өте тұрақты шифрларды алады. Симметриялық криптожүйелердің типтік мысалдары DES, ГОСТ 28-147-89, AES (RIJNDAEL), Camellia стандарттары болып табылады.

Барлық блоктық шифрлар бірнеше режимде жұмыс істей алады:

- ECB (Electronic Code Book) – электрондық кодтық кітап;
- CBS (Cipherblock Chainsng) – шифр блоктарын тіркеу(тізбектеу);
- CFB (Cipher Feedback) – криптомәтін бойынша кері байланыс;
- OFB (Output Feedback) – шығу бойынша кері байланыс.

1.1.3 ECB (Electronic Code Book) – электрондық кодтық кітап

ECB режимінде ашық мәтіннің екілік символдарының тізбегі блоктарға бөлінеді және содан кейін бір кілттің көмегімен оларды тәуелсіз шифрлау жүзеге асырылады (кілттің ұзындығы ашық мәтін блогының ұзындығына сәйкес келеді)[8].

ECB режимінің бірнеше кемшіліктері бар, яғни бір кілттің көмегімен бірдей блоктарды шифрлау нәтижелері сәйкес келеді, криптомәтін (криптограмма) блогының ұзындығы тұрақты және салыстырмалы түрде аз, криптотекстте ұқсас блоктардың болуы сәйкес келетін блоктардың болуына

және ашық мәтіннің тиісті фрагменттеріне анық көрсетуге қызмет етеді, бұл жалпы жағдайда криптоанализді едәуір жеңілдетуі мүмкін.

Екінші жағынан, жіберуші бір кілтпен шифрланған ашық мәтінді екінші рет жіберген жағдайға қатысты екі абонент арасындағы ақпараттық алмасуды бақылау алушы бірінші жағдайда берген сол криптограмма-жауаптың қайтарылуын еліктеуге мүмкіндік береді.

Сонымен, ECB режиміндегі алгоритмдердің көпшілігі қателердің көбеюі деп аталатын қасиетке ие, ол криптограмманың бір битінің бұрмалануы дешифрлеу нәтижесінде алынған ашық мәтінде бірнеше биттің (жартысына жуық) бұрмалануына әкеп соқтырады.

1.1.3 CBS (Cipherblock Chainsng) – шифр блоктарын тіркеу(тізбектеу)

Бұл кемшіліктерді бейтараптандыру үшін CBC деп аталатын арнайы пайдалану режимі (Шифр блоктарының ілінісу режимі) әзірленген.

Бұл режимде M хабары $M_1, \dots, M_n$ блоктарына бөлінеді. Шифрлаудың ағымдағы қадамында ашық мәтіннің әрбір M_i блогына, оны E шифрлау алгоритміне кірер алдында, модуль 2 бойынша қосымша қосу арқылы алдыңғы қадамда алынған шифрленген Mi, шифрланған блогы қосылады. Сондықтан.

$$M_i = E_K(M_i \oplus C_{i-1}) \tag{1.3}$$

Егер екі түрлі хабарлар бірдей блоктармен басталса, онда сәйкес келетін бірінші блоктар тиісті криптомәтіндерге ие болады. Бұл кемшіліктен қорғау үшін әрбір M хабарламасына шифрлау алдында инициализация векторы C_0 деп аталады бастапқы кездейсоқ сан (сан ұзындығы шифрлау блогының ұзындығына сәйкес келеді) беріледі.

Дешифрлау

$$M_i \oplus C_{i-1} = E_K^{-1}(C_i) \tag{1.4}$$

алгоритмі бойынша орындалады немесе

$$M_i = C_{i-1} \oplus E_K^{-1}(C_i). \tag{1.5}$$

Келтірілген қатынастардан көретініміз, әрбір кезекті криптограмма блогы алдыңғысының функциясы болып табылады. Сондықтан криптомәтінде бір биттің бұрмалануы дешифрлау нәтижесінде алынған екі аралас блокты бұрмалайды. Алайда, бұрмаланған криптограмма блогы ашық мәтіннің келесі блогымен жиынтықталғандықтан, келесі шифрланатын блоктағы бұрмалаулар саны криптограммадағы бұрмалаулар санына тең. Криптотөзімділікке келетін болсақ, CBC режимі ECB-дан төзімдірек болып саналады. Оның екі себебі

бар. Біріншіден, криптограмма тек ашық мәтін мен кілттің ғана емес, сонымен қатар C_0 бастапқы векторының да функциясы болып табылады. Бұл, әрине, криптоанализді қиындатады. Екінші жағынан, жалпы мәтіндегі бірдей мәтіндік блоктар әр түрлі криптограмманың блоктарына сәйкес келеді, бұл ECB-нің негізгі кемшіліктерін бейтараптайды.

1.1.4 CFB (Cipher Feedback) – криптомәтін бойынша кері байланыс

Блоктармен операция жасайтын ECB және CBC режимдерінен айырмашылығы (шифрлау блогының ұзындығы сияқты бірдей ұзындық), CFB және OFB режимдері k –биттік блоктармен операция жасайды (ұзындығы 1-ден бірліксіз шифрлау блогының ұзындығына дейін өзгеруі мүмкін). Бұл, атап айтқанда , мәтіндік деректерді бірнеше рет шифрлауға мүмкіндік береді (EBCDIC коды үшін $k = 8$, ал ASCII коды үшін $k = 7$ код)[9].

CFB режимінде базалық алгоритм E шифрлау блогының ұзындығына тең ұзындығы B_i жалған сәулелі биттердің блоктарын құрауға арналған: $B_i = E_K(I_i), \quad i = \overline{0,l},$ мұндағы, $I_0 -$ еркін бастаушы вектор, ал I_{i+1} бірінші I_i битті алып тастау (ауыстыру) және B_{i-1} блогының бірінші (сол жақ) k биттерінің оң жағына қою (толтыру) арқылы алынады. Шифрланған хабар блогы мына түрде беріледі.

$$C_i^{(k)} = m_i^{(k)} \oplus B_i^{(k)}. \qquad (1.4)$$

Мұнда, $C_i^{(k)} - i$-ші шифрлау қадамының k-битті мәтіні; $m_i^{(k)} - k$ битке тиісті ашық мәтін; $B_i^{(k)} - i$-ші қадамда сол жақ k-битті шифрлау нәтижесі; $\oplus$ – модуль 2 бойынша жанама қосу символы.

1.1.5 OFB (Output Feedback) – шығу бойынша кері байланыс.

OFB режимі алдыңғы режимге ұқсас, тек I_i жаңарту үшін B_{i-1} орнына C_{i-1} қолданылады. Көріп отырғанымыздай, CBC режимі сияқты кері байланысы бар блокты шифрлау алгоритмін пайдаланудың қарастырылған екі режимі де ECB басты кемдігінен бос: жалпы жағдайда ашық мәтіннің бірдей блоктарына әртүрлі криптотекст блоктары сәйкес келеді (OFB-ға қатысты, онда бұл бекіту ашық мәтінде саны бірлікке азайтылған қайталану кезеңіне еселенбеген блоктармен бөлінген кез келген бірдей екі блоктарға қатысты болады).

OFB маңызды артықшылығы соңғысын дешифрлау процесінде криптомәтінді беру кезінде орын алған бұрмалаулардың көбею құбылысының болмауы болып табылады. Сонымен қатар, CFB режимінде алынған

криптотексттің k-биттік блогының бір битінің бұрмалануы ашық мәтіннің k-биттік блоктарына бұрмаланған бит дешифрлеу процесінде орындалатын оның мазмұнының жылжу реттілігінің нәтижесінде кіріс блогының шегінен тыс созылғанға дейін әсер етеді.

Блокты шифрлау алгоритмінің және оны пайдаланудың әртүрлі режимдерінің негізгі ерекшеліктері осындай. Ақпараттық жүйелерде берілетін және сақталатын ақпараттың қауіпсіздігін қамтамасыз ету үшін көрсетілген режимдерді қолдану мәселелеріне қысқаша тоқталайық. Әдетте блокты шифрлау алгоритмінің үш саласы қарастырылады:

- деректерді байланыс арналары (ИВС) бойынша беру;
- сақтау;
- ИВС файлдарына (деректер қорына) кіру (доступ);
- коммерциялық ақпарат алмасу.

Байланыс арналарының қауіпсіздігін қамтамасыз ету үшін жоғарыда сипатталған барлық режимдер қолданылуы мүмкін деп саналады, бірақ көптеген аппараттық реализацияны іске асыруда (криптографиялық шифрлау платалары) жанама шифрлауды қамтамасыз ететін $k = 1$ CFB режимі пайдаланылады. Бұл OFB салыстырғанда, әсіресе жоғары жылдамдықты кеңжолақты байланыс арналары негізінде жұмыс істейтін ақпараттық жүйелерге тән бит-бағытталған хаттамаларды криптографиялық қолдау жоспарында оның жоғары криптотөзімділігімен түсіндіріледі. ЭЕМ сыртқы жадында ақпаратты сақтаумен байланысты қосымшаларда қолданудың үш негізгі бағыты бар: тікелей және дәйекті қол жеткізу файлдарын криптографиялық қорғау, сондай-ақ осындай файлдарды жазудың жеке өрістері.

1.2 AES симметриялы блокты криптожүйесінің сипаттамасы

AES симметриялы блокты криптожүйесінің сипаттамасы анықтамалар және көмекші рәсімдер (процедуралар) төмендегі 1.1-кестемен берілген.

1.1 Кесте – AES алгоритмінде айнымалылар анықтамасы[8]

Block	input, output, State және Round Key операцияларынан тұратын бит тізбегі. Сондай-ақ, Block деп байт тізбегін түсінуге болады.
Ciphertext	шифрлау алгоритмінің шығыс деректері
1.1 Кесте жалғасы	
Cipher Key	раунд (Round Keys) үшін кілттер жиынтығын жасауда Key Expansion процедурасын қолданатын құпия, криптографиялық кілт; төрт жолы және N_k колонкалары бар байттардың тікбұрышты массиві ретінде ұсынылуы мүмкін.

Key Expansion	Cipher Key-ден Round Keys генерациясы үшін қолданылатын процедура
Round Key	Round Keys Cipher Key-ден Key Expansion процедурасын пайдалана отырып алынады. Олар шифрлау және дешифрлау кезінде State-ке қолданылады.
State	4 жолы және N_b колонкалары бар байттардың тікбұрышты массиві ретінде ұсынылуы мүмкін шифрлаудың аралық нәтижесі.
S-box	байтты ауыстырудың бірнеше трансформацияларында және Key Expansion процедурасында байт мәнін өзара мәнді ауыстыру үшін қолданылатын ауысудың сызықтық емес кестесі.
N_b	State құрайтын бағандар саны (32 биттік сөздер). AES үшін $N_b = 4$
N_k	шифркілтті құрайтын 32 биттік сөздердің саны. AES үшін $N_k = 4, 6$ немесе 8
N_r	N_k және N_b функциясы болып табылатын раунд саны. AES үшін $N_r = 10, 12, 14$
Rcon[]	32 биттік разрядты сөзден тұратын және осы берілген раунд үшін тұрақты болып табылатын массив

1.2 Кесте – AES алгоритмінде функциялар анықтамасы[9]

AddRoundKey()	Round Key XOR' State-пен шифрлау және кері шифрлау кезіндегі трансформация. RoundKey ұзындығы State өлшеміне тең (N_b= 4 болса , RoundKey ұзындығы = 128 бит немесе 16 байт).
InvMixColumns()	шифрын ашу кезінде MixColumns()-ке кері қатынас болып табылатын трансформация.
InvShiftRows()	шифрын ашу кезінде ShiftRows()-ке кері қатынас болып табылатын трансформация.
1.2 кесте жалғасы	
InvSubBytes()	шифрын ашу кезінде SubBytes()-ке кері қатынас болып табылатын трансформация.
MixColumns()	шифрын ашу кезінде жаңа бағандарды алу үшін барлық State бағандарын алатын және олардың деректерін араластыратын (бір-біріне қарамастан) трансформация.
RotWord()	4 байтты сөзді алатын және оған циклдық алмастыруды жүзеге асыратын Key Expansion процедурасында қолданылатын функция.

ShiftRows()	шифрын ашу кезінде State өңдеу үшін State-тің соңғы үш жолын циклдік әртүрлі шамаларға ығыстыратын трансформация.
SubBytes()	шифрын ашу кезінде әрбір State байтына тәуелсіз қолдана отырып, байттарды алмастырудың сызықты емес кестесін (S-box) пайдалана отырып, State өңделеу кезіндегі трансформация.
SubWord()	кірістерде төрт байт сөзді алатын және төрт байттың әрқайсысына S-box қолдану арқылы шығу сөзін беретін Key Expansion процедурасында қолданылатын функция.

1.2.1 Шифрлау түрлері

AES Rijndael алгоритміне негізделген стандарт болып табылады. AES үшін *input* ұзындығы (кіріс деректер блогы) және State (күйі) тұрақты және 128 битке тең, ал K шифркілтінің ұзындығы 128, 192 немесе 256 бит. Сонымен қатар, Rijndael бастапқы алгоритмі кілттің ұзындығын және блоктың мөлшерін 128-ден 256 битке дейін 32 бит қадаммен жібереді. Таңдалған *input, State* және *Cipher Key* ұзындығын байттарда белгілеу үшін нотация қолданылады. $N_b = 4$ *input* және *State* үшін, $N_k = 4, 6, 8$ *Cipher Key* үшін, сәйкесінше әртүрлі кілттер ұзындықтары үшін.

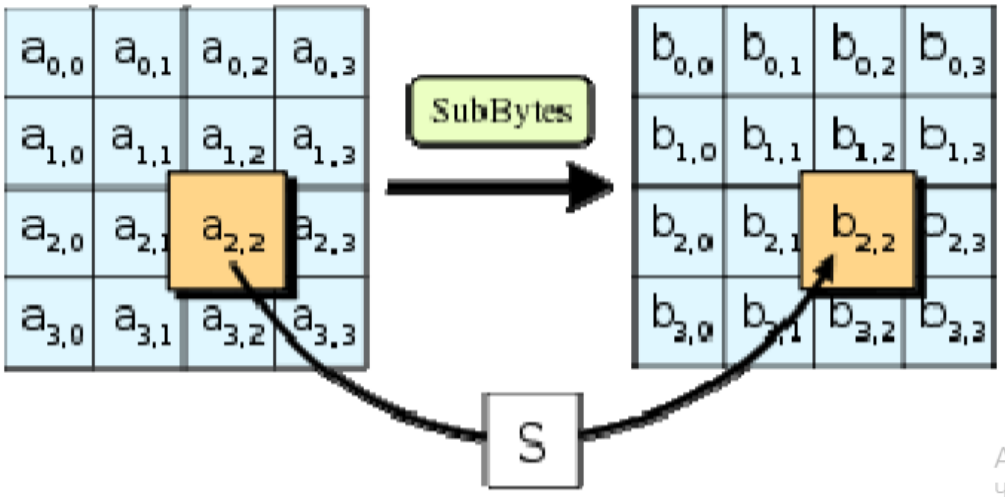
Шифрлау басында *input* ереже бойынша *State* массивіне көшіріледі: $0 \le r < 4$ және $0 \le c < N_b$ үшін $s = [r, c] = in[r + 4c]$. Осыдан кейін *State* AddRoundKey() процедурасы қолданылады, содан кейін *State* 10, 12 немесе 14 рет (кілттің ұзындығына байланысты) трансформация процедурасынан өтеді, бұл ретте соңғы раунды алдыңғылардан бірнеше айырмашылығы бар екенін ескеру қажет. Нәтижесінде, соңғы трансформация раунды аяқтағаннан кейін, *State* мына ереже бойынша *output*-ке көшіріледі: $out[r + 4c] = s[r, c]$ $0 \le r < 4$ және $0 \le c < N_b$ үшін.

Шифр псевдокодта 1 – суретте сипатталған. Жеке трансформациялар *SubBytes(), ShiftRows(), MixColumns(),* және *AddRoundKey()* — *State* өңдейді. Ал, *w[]* массивінің құрамында *key schedule* бар.

Шифрлау алгоритмі:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr-1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
```

end for
SubBytes(state)
ShiftRows(state)
*AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])*
out = state
end
SubBytes()



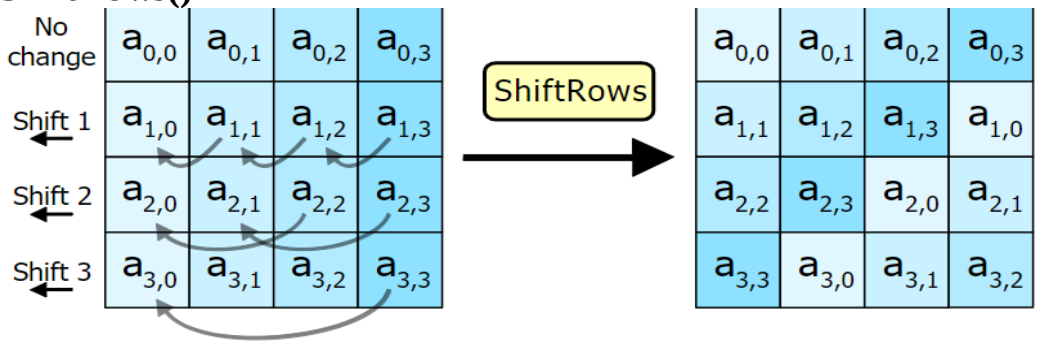
1.1 Сурет – *SubBytes* процедурасы, *State* әрбір байт тіркелген 8 биттік іздеу кестесіндегі тиісті элементпен ауыстырылады, S; $b_{ij} = S(a_{ij})$.

SubBytes() процедурасы S-box көмегімен байттың сызықты емес ауыстырылуын орындайтын әр күй байттарын өңдейді. Бұл операция шифрлау алгоритмінің сызықты еместігін қамтамасыз етеді. S-box құру екі қадамнан тұрады. Біріншіден, $\boldsymbol{GF}(\mathbf{2^8})$ алынған кері сан өндіріледі. Екіншіден, S-box тұратын әрбір b байтқа келесі операция қолданылады: $b_i' = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus b_{(i+7)mod8} \oplus b_i$, мұндағы, $0 \leq i < 8$, $b_i - i$-ші b бит, $c_i - i$-ші c байт, $c = \{63\}$ немесе $\{01100011\}$. Осылайша, қарапайым алгебралық қасиеттерге негізделген шабуылдардан қорғау қамтамасыз етіледі[10].

$$\begin{Vmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix}$$

1.2 Сурет – *Subbytes()* процедурасын матрицалық ұсыну

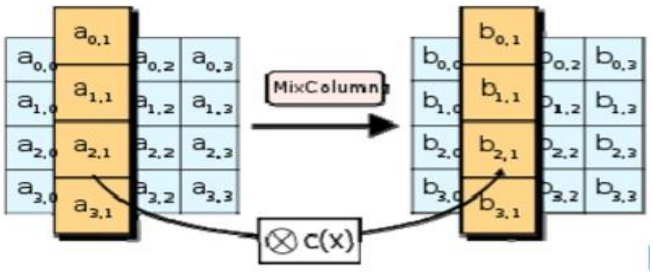
ShiftRows()



1.3 Сурет – ShiftRows процедурасында, байттар state әр жолында циклдік солға жылжиды. Әрбір жолдың байттарының жылжу өлшемі оның нөміріне байланысты

ShiftRows State жолдарымен жұмыс істейді. Бұл трансформация кезінде циклдік күй жолдары жолдың нөміріне байланысты көлденең r байтқа жылжытылады.Нөлдік жол үшін $r = 0$,біріншілік жол үшін $r = 16$ және т.с.с. Осылайша, ShiftRows процедурасын қолданғаннан кейін шығыс күйінің әрбір бағанында бастапқы күйдің әр бағанындағы байттар болады. Rijndael алгоритмінде 128 және 192 биттік жолдар үшін сызықтар бірдей. Алайда, 256 биттік блок үшін ол алдыңғы жолдардан ерекшеленеді, өйткені 2, 3 және 4 жолдар сәйкесінше 1, 3 және 4 байтқа ауысады.

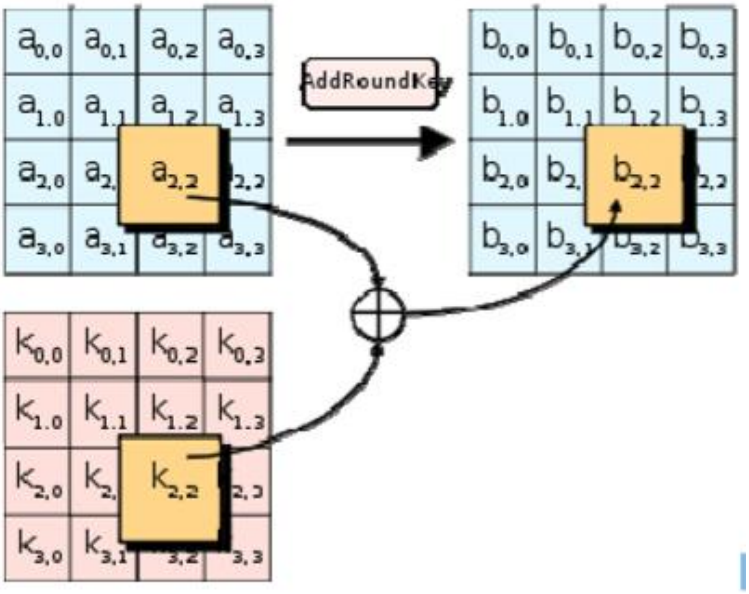
MixColumns()



1.4 Сурет – *MixColumns* процедурасында әр күй бағанасы бекітілген полиномиялық $c(x)$ көпмүшесіне көбейтіледі

MixColumns процедурасында *State* әр бағанасының төрт байты бұл үшін кері сызықтық трансформацияны қолдана отырып араласады. *MixColumns* күйлерін бағандар түрінде өңдейді, олардың әрқайсысын төртінші дәрежелі көпмүшелік (полином) ретінде қарастырады. Бұл көпмүшелер $\boldsymbol{GF(2^8)}$ $x^4 + 1$ модулінде тұрақты көпмүшеге (полиномға) көбейтіледі $c(x) = 3x^3 + x^2 + x + 2$. *ShiftRows*, *MixColumns* бірге шифрға диффузияны енгізеді.

AddRoundKey()



1.5 Сурет – *AddRoundKey* процедурасында әрбір күй байты XOR operation ($\oplus$) арқылы *RoundKey*-мен біріктіріледі

AddRoundKey процедурасында RoundKey әр раундта State-пен біріктіріледі. Әрбір Roundkey кезеңі үшін KeyExpansion процедурасын пайдалана отырып CipherKey шығады; әрбір RoundKey State сияқты бірдей өлшемде. Процедура әр State-тің әр байтынан әрбір RoundKey байтпен аздап биттік XOR шығарады (өндіреді)[11].

KeyExpansion()

AES алгоритмі *KeyExpansion()* процедурасын қолданып және оны *Cipher Key, K* шифрлы кілтпен қамтамасыз ете отырып, барлық айналымдар үшін кілттерді алады. $N_b(N_r+1)$ сөзі: бастапқыда алгоритм N_b сөздерінің жиынтығын талап етеді, ал N_r айналымының әрқайсысы N_b кілтінің жиынтығын қажет етеді. Раундтарға арналған кілттердің алынған массиві $w[i]$, $0 \le i < N_b(N_r+1)$ ретінде белгіленеді. *KeyExpansion()* алгоритмі жалған кодта (псевдокод) 6 – суретте көрсетілген.

SubWord() функциясы төртбайттық кіріс сөзін алады және S-box-ты төрт байттың әрқайсысына қолданады, содан соң барлығын шығысқа жібереді. $[a_0, a_1, a_2, a_3]$ сөзі *RotWord()* кірісіне беріледі, ол циклды түрде қайта құрылып, қайтарылады $[a_1, a_2, a_3, a_0]$. Сөздердің жиыны, берілген айналым үшін тұрақты болатын сөздер, *Rcon [i]*, ол мына мәндер жиынын қамтиды: $[x^{i-1}, 00, 00, 00]$, мұндағы $x = \{02\}$, ал x^{i-1} –х-тің $GF(2^2)$-дегі (i 1 – ден басталады) дәрежесі.

Суреттен кеңейтілген кілттің алғашқы N_k сөздері шифр кілтімен *Cipher Key* толтырылғанын көруге болады. Әрбір келесі сөзге, $w[i]$, XOR операциясы кезінде алынған мән алынады $w[i-1]$ және $w[i-N_k]$, сол XOR' алдыңғы және N_k позицияларға сөзден бұрын тұрады. Позициясы N_k еселігі бар сөздер

үшін XOR алдында $w[i-1]$, содан кейін тұрақты Rcon [i] болатын XOR трансформация қолданылады. Жоғарыда көрсетілген трансформация *RotWord()* сөзіндегі байттардың циклдық жылжуынан тұрады, одан кейін *SubWord()* процедурасы *SubBytes()* сияқты тек кіріс және кіріс деректері сөз өлшемінде болады.

256 биттік *Cipher Key* шифрлау кілті үшін *KeyExpansion()* процедурасы 128 және 192 биттік криптографиялық кілттер үшін қолданылатын процедурадан сәл ғана өзгеше. Егер $N_k = 8$ және $i - 4$ N_k еселік (көбейтінді) болса, онда *SubWord()* XOR' дейін $w[i-1]$ қолданылады[11].

Кілтті кеңейту алгоритмі:

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
word temp
 i = 0;
while ( i < Nk)
        w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
         i = i+1
end while
 i = Nk
while ( i < Nb * (Nr+1))
        temp = w[i-1]
        if (i mod Nk = 0)
                temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
        else if (Nk > 6 and i mod Nk = 4)
                temp = SubWord(temp)
        end if
        w[i] = w[i-Nk] xor temp
        i = i + 1
end while
end
```

Шифрды ашу

Шифрды ашу алгоритмі:

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 step -1 downto 1
        InvShiftRows(state)
        InvSubBytes(state)
        InvAddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
        InvMixColumns(state)
end for
InvShiftRows(state)
InvSubBytes(state)
InvAddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

Алгоритм нұсқалары:

AES негізінде жатқан Rijndael алгоритмі негізінде альтернативті криптоалгоритмдер іске асырылды. Ең танымал Nessie конкурсының қатысушылары: Anubis авторы Винсент Рэймен және шифрдың күшейтілген нұсқасы — Grand Cru Йохан Борст.

1.3 Шифрлық криптологияны іске асыру жақандық ерекшеліктері

AES шифрлау стандарты симметриялық шифрлау үшін АҚШ үкіметінің ресми стандарты болып табылады. Стандарт FIPS #197 (2001) жариялаумен (публикация) анықталады және өнімділігі мен қауіпсіздігіне жоғары талаптар қойылатын түрлі қосымшаларда қолданылады.

Intel компаниясы осы фирманың келесі процессорларының ұрпағында іске асырылатын "бірнеше деректерге арналған бір нұсқаулық" (SIMD, Single Instruction Multiple Data) түріндегі командалардың жаңа жиынтығын ұсынды. Бұл нұсқаулар AES алгоритмі арқылы жылдам және қауіпсіз шифрлау мен дешифрлауды қамтамасыз етеді.

SSE деп аталатын бұл командалар жиынтығы (Streaming SIMD Extensions, ағынды SIMD кеңейту) алты нұсқаулықты қамтиды. Олардың төртеуі – AESENC, AESENCLAST, AESDEC және AESDELAST жоғары сапалы шифрлауды және шифрлауды қамтамасыз етеді. Тағы екеуі, AESIMC және AESKEYGENASSIST, AES кілтін кеңейтуді жасауға мүмкіндік береді. Бірлесе отырып, олар AES стандарты үшін қауіпсіздіктің, өнімділіктің және икемділіктің қажетті деңгейімен толық қамтамасыз етеді. Бұл мақала AES алгоритміне шолу және жоғары өнімділік пен шифрлау қауіпсіздігіне жету үшін оның нұсқауларын пайдалану әдістеріне әкеледі. Осы алгоритмді арнайы қолданудың кейбір мысалдары келтірілген.

1.3.1 AES және Intel® архитектурасы

AES шифрлау стандарты симметриялы шифрлау үшін АҚШ үкіметінің ресми стандарты болып табылады және FIPS №197 (FIPS197 hereafter) жарияланымында сипатталған.

AES 128 биттік шифрланған блокта 128 биттік мәтіндік блокты кодтайтын блокты шифр болып табылады немесе 128 биттік шифрланған блокты 128 биттік мәтіндік блокта дешифрлайды.

AES-128, AES-192, AES-256 деректер блоктарын тиісінше 10, 12 немесе 14 итерация бойынша өңдейді. Әрбір итерация – трансформацияның белгілі бір тізбегі. Барлық итерациялар бірдей болады, тек соңғы өзгертулерден басқа, яғни қайсыбір түрлендірулер алынып тасталады. Алдағы уақытта біз итерацияны раунд деп атаймыз.

Әрбір раунд екі 128 биттік блоктармен жұмыс істейді: "ағымдағы" және "раунд кілті". Барлық раундтар әр түрлі "раунд кілттерін" қолданады, олар кілтті кеңейту алгоритмі арқылы алынады. Бұл алгоритм шифрланған деректерге байланысты емес және шифрлау/дешифрлау фазасына қарамастан орындалуы мүмкін.

Деректер блогы келесі кезеңдерден өтеді: оның үстінде бірінші 128 биттік кілттер XOR операциясы орындалады, шығыста "ағымдағы" блок шығады(бұл кезең нөлдік раунд деп те аталады, нөлдік раунд батырма – шифрлық кілттің алғашқы 128 биті). Содан кейін ағымдағы блок 10/12/14 шифрлау раунды арқылы өтеді, содан кейін ол шифрланған (немесе дешифрланған) блокқа айналады.

1.3.2 Байт орналасуы: Little Endian Intel архитектурасы және Big Endian FIPS197 спецификациясы

GSM (Groupe Spécial Mobile (Мобильді Арнайы Топ) тобының атауынан кейін Global System for Mobile Communications (Жаһандық ұялы байланыс жүйесі) деп аталды. Жаһандық стандарты цифрлық ұялы байланыс бөле отырып арналарды уақыт (TDMA) және жиілік (FDMA) деп бөлді[13].

1.4 GSM ұялы стандартының криптографиялық алгоритмдерін енгізу

GSM-әлемдегі ең кең қолданылатын ұялы стандарт. Ұялы желі - бұл ортақ ақпарат құралын кез келген пайдаланушы желіге кедергі жасай алады. Тасымалдаушы құрал ортақ болғандықтан кез-келген пайдаланушы ақпаратты тыңдай алады немесе жібере алады. Сондайақ байланыс жүйесі жекеш таратылмайды. Ортақ тарату құралын пайдаланған кезде қандай да бір ақпарат қаупсіздігін қорғайтын әдіс орнатылмаса, онда жеке құпиялық сақталмауы мүмкін. Криптографиялық сақтық пен жеке меншік ақпаратың қауіпсіздігін бақылауды қалпына келтіруге мүмкіндік береді. A5/x - GSM ұялы телефондарындағы сөйлесулердің құпиялығын қамтамасыз ету үшін қолданылатын шифрлау алгоритмдері. Кеңестік интерфейсі арқылы жіберілетін ақпараттарды қорғау үшін A5/x алгоритмдері. A5/1 жақсы нұсқасы көптеген елдерде қолданылады. A5/2 - экспортқа шектеулер қолданылатын елдерде қолданылған әлсіз нұсқа. A5/3 шифрлау алгоритмі GSM және ECSD және GPRS үшін шифрлау алгоритмі үшін қолданылады.

Менің дипломдық жұмысым A5/1 және A5/3 алгоритмдерін модельдеуге негізделген[14].

Ұялы байланыстағы шифрлау абоненттердің ақпаратын қорғау және алаяқтықтың алдын алу үшін өте маңызды. GSM жүйесінде құпиялылық пен қауіпсіздікті қамтамасыз етудің әртүрлі әдістері бар. Құпия кілттердің криптографиялық жүйелерін блоктық немесе ағындық шифрларға жіктеуге болады. *Блоктық шифрларлау* - құпия емес кілттің әсерінен жай мәтіндік мәліметтердің N-биттік блоктарын өзгертіп, шифрланған мәліметтердің N-блоктарын құратын алгоритмдер. *Ағын шифрлау* ішкі күйлерден тұрады және жалған кездейсоқ кілттердің ағындарын генерациялау арқылы жүйелі түрде жұмыс істейдтін негізгі ағын (ағынды шифрлау негізгі генераторлар деп аталады). Ағындық шифрлау блоктықтардағыдай қателіктердің таралуына ұшырамайды, өйткені әр бит өздігінен шифрланады және дишифрланады. Олар әдетте блок шифрларына қарағанда әлдеқайда жылдам және бағдарламалық қамтамасыздандырудың тиімділігі жоғары.

GSM қауіпсіздік қабатында 64 биттік құпия кілтте қолданатын A5 ағынды шифрлау әдісі қолданылады. A5/1 және A5/2 нұсқалары ұзақ уақыт құпия болды. GSM A5 алгоритмі әзірленгендіктен, криптографияның жалпы жағыдайы айтарлықтай өзгерді [15]. Жақында Briceno және тағы басқалар A5/1 және A5/2 GSM жүйесінен кері құрастырылды телефон шығарды. Сондада A5/2 криптолгиялық талдау нәтижесі толықтай қауіз болмады.

Өте аз кездейсоқ шабуылдан сақтану үшін 216 қадамды қажет етті. A5/3 деп аталатын жаңа қауіпсіздік алгоритмі GSM ұялы телефондарының пайдаланушыларын ұрлап тыңдаудан қорғаудың жоғары деңгейімен қамтамасыз етеді[15]. A5/3 GSM жүйелерінде қолдану үшін GSM қауымдастығының қауіпсіздік тобы мен 3-ші буын серіктестік жобасы арасындағы бірлескен жұмыс тобымен жасалды. Ол сондай-ақ General Packet Radio Service (GPRS) үшін қолданылады, онда ол GEA3 ретінде белгілі болады, сонымен қатар GSM Evolution (EDGE) үшін кеңейтілген деректер жылдамдығында GSM Evolution (EDGE) үшін жетілдірілген деректер жылдамдығы сияқты басқа GSM режимдері қолданылады [16]. A5/3 шифрлау алгоритмі сигналдық қорғанысты қамтамасыз етеді, осылайша телефон нөмірлері сияқты құпия ақпарат радиосигналдық жол арқылы қорғалады және пайдаланушының деректерін дауыстық қоңырауларын және радиосигнал арқылы өтетін басқа да пайдаланушылар жасаған деректерді қорғауға мүмкіндік береді [16]. A5/3 және GEA3 алгоритмдері Mitsubishi негізгі патенттеріне ие 3GPP шифрлау алгоритміне негізделген.

1.4.1 Ұялы байланыста қолданылатын негізі криптографиялар

A5/1 - GSM ұялы телефон стандартында сымысыз байланыстан басқа байланыстың құпиялығын қамтамасыз ету үшін қолданылатын ағындық шифрлау әдісі. Бұл GSM-де қолдану үшін көрсетілген жеті алгоритмнің бірі. Бастапқыда бұл құпия сақталды, бірақ ақпаратың таралып кетуі және кері инженерия арқылы көпшілікке мәлім болды. Шифрлаудада бірқатар елеулі кемшіліктер анықталды.

1.4.2 A5 шифрлау алгоритмі

A5-бұл GSM (Groupe Spécial Mobile) еуропалық ұялы сандық байланыс жүйесінде телефон мен базалық станция арасында берілетін деректердің құпиялылығын қамтамасыз ету үшін қолданылатын шифрлаудың ағымдық алгоритмі.

Шифр екі модуль бойынша (булева операция "жоқ//немесе") жалған сәулеленетін жүйелілік пен шифрленетін ақпарат бойынша жанама қосылымға негізделген. A5 жалған кездейсоқ тізбектегі кері байланыс арқылы үш сызықты жылжу регистрі негізінде жүзеге асырылады. Регистрлердің ұзындығы тиісінше 19, 22 және 23 бит. Қозғалыстар әрбір қадамда кем дегенде екі Регистр ығысуын ұйымдастыратын арнайы схеманы басқарады, бұл олардың біркелкі қозғалуына әкеледі. Реттілік регистрлердің шығу биттерінен "болдырмайтын немесе" операциялары арқылы қалыптасады[17].

Құрылу және даму тарихы. Бастапқыда француз әскери мамандар-криптографтар тек әскери мақсатта пайдалану үшін ағынды шифр әзірледі. 80 соңында GSM стандарты үшін жаңа, заманауи қауіпсіздік жүйесін құру қажет болды. Оның негізі үш құпия алгоритм болды: аутентификация — A3, ағынды шифрлау — A5, сеанстық кілтті генерациялау — A8. A5 алгоритмі ретінде француз әзірлемесі қолданылды. Бұл шифр ағынның жақсы қорғанысын қамтамасыз етті, демек, сөйлесудің құпиялылығын қамтамасыз етті. Бастапқыда Еуропадан стандарт экспорты болжанбаған, бірақ көп ұзамай бұл қажеттілік пайда болды. Сол себепті A5 A5/1 атауын өзгертіп, Еуропада да, АҚШ-та да тарата бастады. Басқа елдер үшін (соның ішінде Ресей) алгоритм шифрдың криптотөзімділігін айтарлықтай төмендетіп модификациялады. A5/2 Еуроодаққа кірмейтін елдер үшін экспорттық нұсқа ретінде арнайы әзірленген. Криптостойкость A5/2 понижена қосылған тағы бір тіркелімінің (17 бит), басқарушы сдвигами қалған. A5/0 шифрлау мүлдем жоқ. Қазіргі уақытта Касуми алгоритміне негізделген және 3G желілерінде пайдалану үшін бекітілген A5/3 алгоритмі әзірленді.

Кең қолжетімділікте пайда болуы. Ресми түрде бұл криптосхема жарияланбаған және оның құрылымы жариялауда болмады. Бұл әзірлеушілер беймәлімділік салдарынан қауіпсіздікке сүйенгенімен байланысты болды, егер

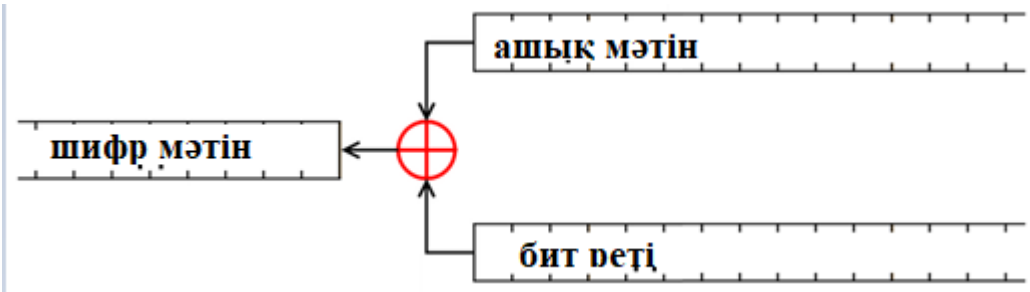
олардың сипаттамалары көпшілікке қол жетімді болмаса алгоритмдерді бұзу қиын. Деректер GSM операторларына қажет болған жағдайда ғана берілді. Дегенмен, 1994 жылға қарай A5 алгоритмінің бөлшектері белгілі болды: British Telecom Британдық телефон компаниясы ақпаратты жарияламау туралы келісім жасамай, талдау үшін Брэдфорд университетіне стандартқа қатысты барлық құжаттарды берді. Сонымен қатар, стандарт туралы материалдар Қытайда конференциялардың бірінде пайда болды. Нәтижесінде оның схемасы біртіндеп көпшілікке қосылды. Осы жылы Кембридж ғалымдары Росс Андерсон (Ross Anderson) және Майкл Роу (Michael Roe) осы деректер бойынша қалпына келтірілген криптосхеманы жариялап, оның криптотөзімділігіне баға берді[1]. Қорытынды алгоритм Eurocrypt 97 конференциясында Йована Голичтің жұмысында ұсынылды.

A5 құрылымы**.** Қазіргі уақытта A5 алгоритмі-шифрлардың тұтас тобы. Сипаттама үшін бұл топтаманың ең алғашқысы ретінде A5/1 болады. Туынды алгоритмдердегі өзгерістерді бөлек сипаттаймыз[17].

1.4.3 Ағынды шифрлау

Ағындық немесе ағындық шифр — бұл симметриялық шифр, онда ашық мәтіннің әрбір символы пайдаланылатын кілтке ғана емес, оның ашық мәтін ағысындағы орналасуына байланысты шифрланған мәтін символына айналады. Ағындық шифр блоктық шифрларға қарағанда симметриялық шифрлаудың басқа тәсілін жүзеге асырады.

Бұл алгоритмде әрбір ашық мәтіннің символына шифр мәтіннің символы сәйкес келеді. Мәтін блоктарға (блоктық шифрлау сияқты) бөлінбейді және көлемі өзгермейді. Аппараттық іске асыруды оңайлату үшін және, демек, жылдам әрекетті арттыру үшін тек қарапайым операциялар қолданылады: 2 (XOR) модулі бойынша қосу және тіркелімді ауыстыру[18].



1.6 Сурет – Ағымдық шифр схемасы: ашық мәтінді қосу және бит кезектілігі шифрмәтін береді

Шығыс реттілігін қалыптастыру бастапқы мәтін ағынын генерацияланатын тізбектілікпен (гаммамен) қосу арқылы жүзеге асырылады. XOR операциясының ерекшелігі-қолданылған жұп сан бастапқы мәнге

әкеледі. Демек, хабарламаны декодтау белгілі бір бірізділікпен шифротекстті қосу арқылы жүзеге асырылады.

Осылайша, жүйенің қауіпсіздігі жүйелілік қасиеттеріне толық байланысты. Әрбір бит гамма - тәуелсіз кездейсоқ шама, және тізбектің өзі кездейсоқ. Мұндай схема 1917 жылы Вернам ойлап тапты және оның құрметіне аталды. 1949 жылы Клод Шеннон дәлелдеді, бұл абсолютті криптотөзімді қамтамасыз етеді. Бірақ кездейсоқ бірізділікті пайдалану ашық мәтінге тең, қорғалған арна бойынша хабар беруді білдіреді, бұл тапсырманы айтарлықтай қиындатады және іс жүзінде еш жерде қолданылмайды.

Нақты жүйелерде берілген өлшемнің кілті жасалады, ол жабық арна бойынша қиындықсыз беріледі. Тізбек оның негізінде жасалады және жалған кездейсоқ болып табылады. Үлкен класты ағындық шифр (оның ішінде А5) шифр, жалған кездейсоқ тізбектің генераторы құрайды[19].

1.4.5 А5 алгоритмінің жұмыс істеуі

Белгілі схема негізінде алгоритмнің жұмыс істеу ерекшеліктерін қарастырайық. Мәліметтерді жіберу құрылымдалған түрде — кадрларға бөле отырып (114 бит) жүзеге асырылады. Инициализация алдында регистрлер нөлденеді, кіру алгоритміне сеанс кілті түседі (К – 64 бит) қалыптастырылған А8, және кадр нөмірі (Fn – 22 бит). Бұдан әрі келесі әрекеттер жүйелі түрде орындалады:

* Инициализациялау:

- 64 такт, онда XOR кілтінің әрбір регистрлердің кіші битімен кезекті бит жылжиды, бұл ретте регистрлер әр тактте жылжиды,
- ұқсас 22 такт, тек XOR операциясы кадр нөмірімен жүргізіледі,
- 100 такт регистрлердің жылжуын басқарумен, бірақ тізбекті генерациялаусыз,

• 228 (114 + 114) жұмыс тактары, берілетін кадрды шифрлау (алғашқы 114 бит) және қабылданатын шифрды шифрлеу (соңғы 114 бит) жүргізіледі.,

* бұдан әрі инициализация қайтадан жүргізіледі, кадрдың жаңа нөмірі қолданылады[20].

1.4.6 А5/х туындысының айырмашылығы[20].

А5/2 алгоритміне басқалардың қозғалысын басқаратын 17 битке (R4) тағы бір регистр қосылды. Құрылымның өзгеруі келесідей:

* Ұзындығы 17 бит R4 регистрі қосылды,

* R4 үшін кері байланыс көп: ,

* тактілеуді басқару R4 жүзеге асырады. R4 биттер 3, 7, 10 синхрондау биттері бар.

- мажоритарлы функция F = x&y|x&z|y&z (көпшілігіне тең), мұнда булево AND, булево OR, ал x, y және z синхрондау биттері R4(3), R4(7) және R4(10) сәйкесінше есептеледі,
- R1, R4(10) = F болса жылжытылады,
- R2, егер R4(3) = F болса жылжытылады,
- R3, R4(7) = F болса жылжытылады,

* жүйенің шығыс биті - регистрлердің үлкен биттері мен мажоритарлық функцияларды регистрлердің белгілі бір биттерінен XOR операциясының нәтижесі:

- R1 — 12, 14, 15,
- R2 — 9, 13, 16,
- R3 — 13, 16, 18.

Жұмыс істеудегі мұндай өзгерістер маңызды емес және тек инициализацияға қатысты:

* 64+22 такт сеанстық кілтпен және кадр нөмірімен де R4 толтырылады, 1 такт R4(3), R4(7) және R4(10) 1 толтырылады, 99 такт регистрлердің жылжуын басқарумен, бірақ тізбекті генерациялаусыз.Инициализация сол уақытты алатыны көрінеді. (генерациясыз 100 тактілер екі бөлікке бөлінген).

A5/3 алгоритмі 2001 жылы әзірленді және ұялы жүйелердің үшінші буынында A5/1-ді ауыстыруы тиіс. Сондай-ақ, ол Касуми алгоритмі деп аталады. Оны құру кезінде Mitsubishi корпорациясының MISTY шифры негізге алынды. Қазіргі уақытта A5/3 талап етілетін беріктікті қамтамасыз етеді деп саналады. A5/0 алгоритмінде шифрлау жоқ.

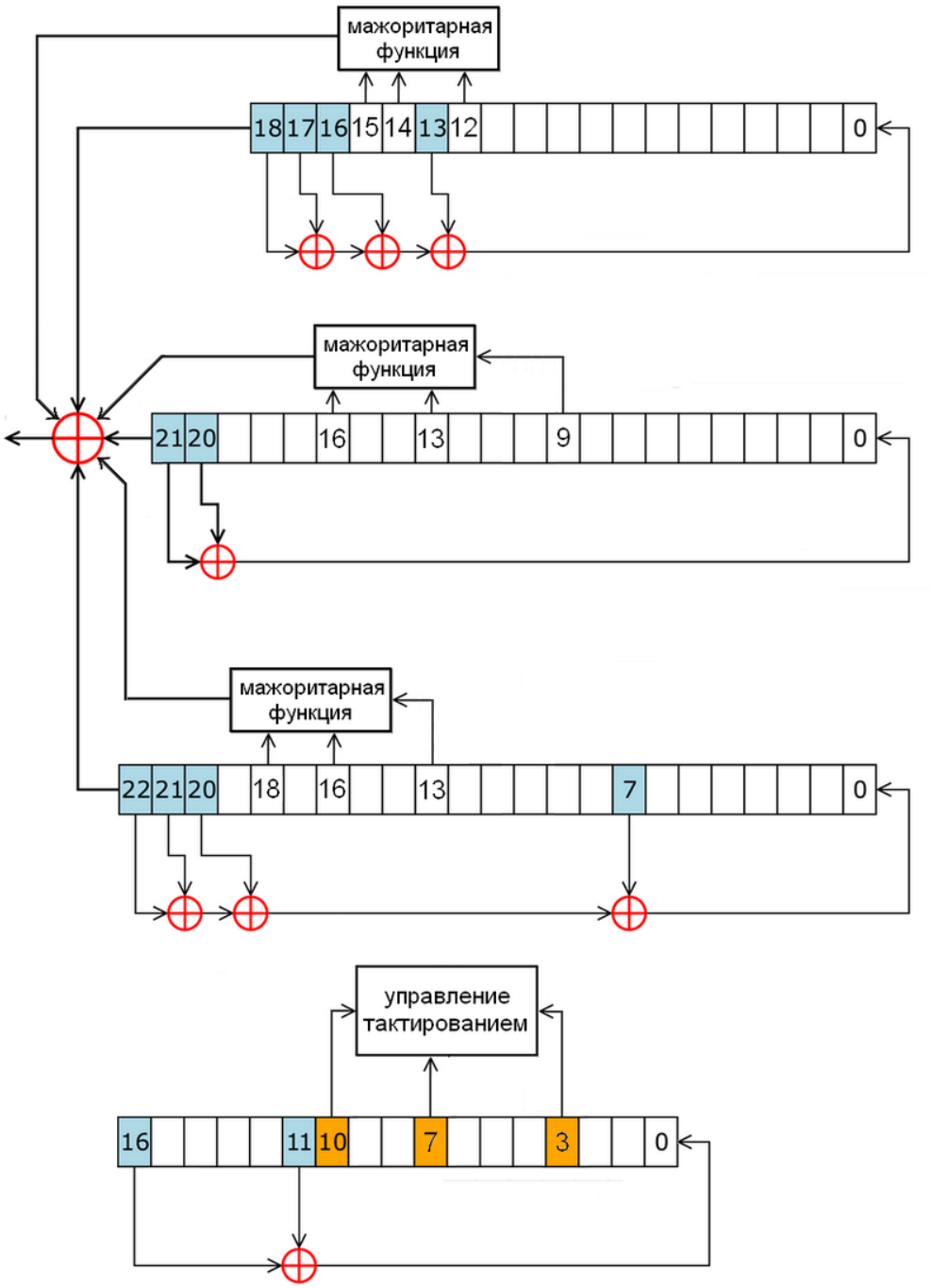
GSM стандартын әзірлеу, бұл бұзылмайтын шифрлаудың қуатты аппаратын білдіреді (әсіресе нақты уақытта). Іске асыру кезінде пайдаланылатын әзірлемелер берілетін деректерді сапалы шифрлауды қамтамасыз етті. Бұл стандартты таратын компаниялардан дәл осындай ақпаратты алуға болады. Бірақ маңызды нюансты атап өту керек: сөйлесулерді тыңдау-арнайы қызметтер пайдаланатын ажырамас атрибут. Олар өз мақсаттары үшін телефон сөйлесулерін тыңдау мүмкіндігіне мүдделі болды. Осылайша, алгоритмге қолайлы уақытта бұзуға мүмкіндік беретін өзгерістер енгізілді. Бұдан басқа, A5 экспорты үшін A5/2 түрлендірілді. MoU-да (Memorandum of Understand Groupe Special Mobile standard) A5/2 әзірлеу мақсаты шифрлаудың криптотөзімділігі төмендегенін мойындайды, алайда тестілеудің ресми нәтижелерінде алгоритмнің қандай да бір кемшіліктері белгісіз.

A5 стандарты туралы деректердің пайда болуымен алгоритмді бұзу, сондай-ақ осалдықтарды іздеу әрекеттері басталды. Қорғауды күрт әлсірететін стандарттың ерекшеліктері үлкен рөл атқарды, атап айтқанда:

- 10 бит кілті мәжбүрлі бос,
- тіркемелер арасында айқас байланыстардың болмауы (жылжуды басқарудан басқа),
- криптоаналитикке белгілі қызметтік ақпаратты шифрлау,

- 40% - дан астам кілттер кезеңнің ең аз ұзындығына әкеледі, нақтырақ $\frac{4}{3}(2^{23}-1)$ болады[21].
- сеанс басында нөлдік хабарлама алмасу жүзеге асырылады (бір кадр бойынша),
- барлық пакеттер үшін бірдей қосымша (padding) ,
- A5/2-де қозғалыс ұзындығы 17 бит жеке Регистр арқылы жүзеге асырылады.

Осы "тесік" негізінде алгоритмде бұзу схемалары салынған.



1.7 Сурет – A5/2 алгоритміндегі регистрлер жүйесі

Белгілі шабуылдардың болуы**.** Кілт болып 64 биттің ұзындықты сеанс кілті табылады, кадр нөмірі белгілі болып саналады. Осылайша, тікелей аралыққа негізделген шабуылдың күрделілігі 264 тең.

Шифрдің алғашқы шолуы (Росс Андерсонның жұмысы) алгоритмнің осалдығын бірден анықтады — кілттің тиімді ұзындығының азаюынан (10 бит нөлденуі) күрделілік 245-ке дейін төмендеді (бірден 6 рет). Андерсонның шабуылы қысқа регистрлерді бастапқы толтыру туралы болжамға және үшінші толтыру алудың шығу деректері бойынша негізделген.

1997 жылы Йован Голич A5 талдауының нәтижелерін жариялады. Ол 64 бит ұзындығы бар гамманың белгілі бөлігі бойынша регистрлердің бастапқы толтырылуын анықтау тәсілін ұсынды. Бұл бөлік нөлдік хабарламадан алынады. Шабуылдың орташа күрделілігі 240.

1999 жылы Вагнер мен Голдберг жүйені ашу үшін R4 бастапқы толтырылуын барынша аралықпен анықтау жеткілікті екенін оңай көрсете алды. Тексеру нөлдік кадрлар есебінен жүзеге асырылады. Бұл шабуылдың күрделілігі 217-ге тең, осылайша, қазіргі заманғы компьютерде шифрді ашу бірнеше секундқа созылады[22].

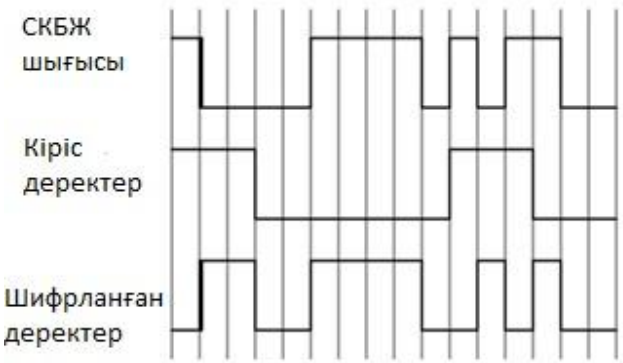
1999 жылдың желтоқсанында израильдік ғалымдар тобы (Ади Шамир, Алекс Бирюков, кейінірек американдық Дэвид Вагнер (ағылш.) өте жақсы емес, бірақ теориялық тұрғыдан өте тиімді ашу әдісін A5/1 жариялады [22].

2 Ұялы байланыс жүйесіне қолданылатын криптологиялық шифрлау технологясы

2.1 Сызықтық кері байланысы бар жылжу регистрі құрылымы

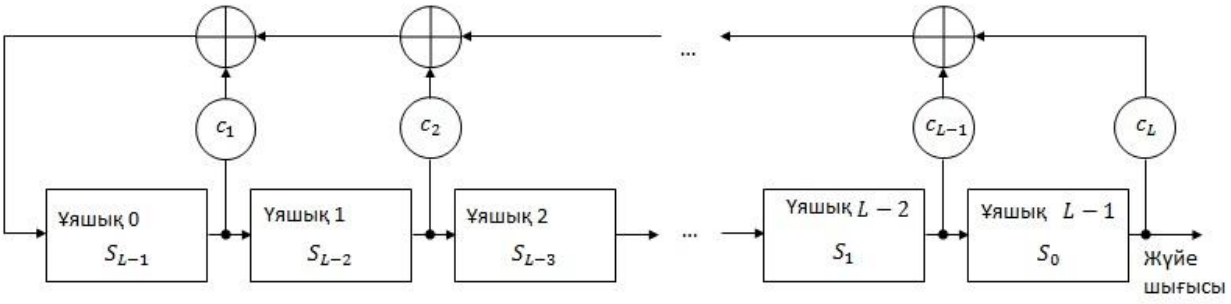
Сызықтық кері байланысы бар жылжу регистрінде (СКБЖР) екі бөлік (модуль) бөлінеді: жылжу регистрі; кері байланыс схемасы (немесе кіші бағдарлама), жылжитын биттің мәнін есептеу[23].

Сызықтық кері байланысы бар жылжу регистрі (СКБЖР, ағылш. linear feedback shift register, LFSR) - биттік сөздердің жылжу регистрі, оның кіріс битінің мәні регистрдің қалған биттерінің мәндерінен бастап жылжытуға дейінгі сызықтық түйреуіш функциясына тең. Бағдарламалық және аппараттық құралдармен ұйымдастыру үшін қолданылады, генерациялаудан алынған кездейсоқ тізбекті биттерды қолдану криптологясы. Төменде сызықтық кері байланысы бар жылжу регистрі СКБЖР құрылым көрсетілген



2.1 Сурет – Сызықтық кері байланысы бар жылжу регистрі және СКБЖР көмегімен деректерді шифрлау схемасы

Регистр функциялық жад ұяшықтарынан (бір немесе бірнеше машиналық сөздердің биттерінен) тұрады, олардың әрқайсысында бір биттің ағымдағы күйі (мәні) сақталады. L ұяшықтарының саны регистрдің ұзындығы деп аталады. Биттер (ұяшықтар) әдетте i сандармен нөмірленед i=0,1….,L-1 ұяшықтың мазмұны $S_{(L-1)-i}$ арқылы белгіленеді(2.1-сурет). Жаңа бит мәні S_L бит регистрде жылжытқанға дейін анықталады және тек жылжытқаннан кейін ғана 0 ұяшығына жазылады, ал L-1 ұяшығынан кезекті генерацияланған бит алынады.



2.2 Сурет – Сызықты кері байланысы бар жылжу регистрі тіркеу жұмысы

СКБЖР үшін кері байланыс функциясы регистрдің барлық немесе кейбір биттерінің мәндеріне қолданылатын сызықтық Булев функциясы болып табылады. Функция регистрдің биттерін c_i коэффициенттеріне көбейтуді орындайды, мұнда i=1,2,…., L. коэффициенттер саны L регистрінің биттер санымен сәйкес келеді. Сі коэффициенттері мәнін қабылдайды $\{0, 1\}$, сонымен бірге, соңғы коэффициент C_L=1 тең, өйткені СКБЖР L сипаттамалық көп мақсатты дәрежеге қойылады.

Модуль бойынша қосу (формулаларда символымен белгіленетін "XOR" операциясы) немесе оның логикалық инверсиясы "XNOR" сызықтық Булев функциялары болып табылады және мұндай регистрлерде жиі қолданылады[24]. Сонымен қатар, кері байланыс функциясының айнымалы болып табылатын биттер кері бұрулар деп аталады,ал регистр Фибоначчи конфигурациясы деп аталады. Аппаратты іске асыруларда тіркелімді басқару барлық ұяшықтарға жылжитын импульсті (тактикалық немесе синхроимпульс деп аталатыннан басқа) беру арқылы жүргізіледі. Регистрді бағдарламалық іске асыруда басқару циклді орындаумен жүргізіледі. Циклдың әр итерациясында кері байланыс функциясы есептеледі және сөзде биттерді жылжыту орындалады.

2.2 Сызықтық кері байланысы бар жылжу регистрының жұмыс істеу принципі

Әрбір такты ішінде сызықтық кері байланысы бар жылжу регистрі келесі операцияларды орындайды. L-1 ұяшығында орналасқан бит оқылады;

- кері байланыс функциясы ағымдағы ұяшықтар мәндерін пайдалана отырып, 0 ұяшығы үшін жаңа мәнді есептейді;
- әрбір і ұяшықтың мазмұны келесі ұяшыққа өтеді і+1, мұнда і=0,1, L-2;
- 0 ұяшығына бұрын Кері байланыс функциясымен есептелген бит жазылады.

Егер кері байланыс функциясы "XOR" (немесе) логикалық әрекетін орындаса, бит (ұяшықтар) мәндері келесі формулалар бойынша есептелінеді:

$$S_L = (c_1 * S_{L-1}) + (c_2 * S_{L-2}) + \cdots + c_L * S_0) \quad (2.1)$$

$$S_{L+1} = (c_1 * S_L) + (c_2 * S_{L-1}) + \cdots + c_L * S_1) \ldots \quad (2.2)$$

$$S_{L+j-1} = (c_1 * S_{L+j-2}) + (c_2 * S_{L+j-3}) + \cdots + c_L * S_{j-1}) \quad (2.3)$$

Жылжу регистрінің кезеңі оны қайталау басталғанға дейін алынатын кезектіліктің ең аз ұзындығы деп аталады. L ұзындығыны СКБЖР ұяшықтарда бит мәнін беретін 2^L бастапқы күйге ие. Олардың 2^{L-1} күйі - нөлдік емес, сондықтан генерацияланатын тізбектің $T \leq 2^{L-1}$ кезеңі бар[25]. GF2 өрісінің үстінде қарапайым. Бұл үшін келесі 2 шартты орындау қажет (бірақ жеткілікті емес):

Бұрудың жұп саны. бұрылыстар нөмірлері, барлығы бірге емес, өзара қарапайым. Барлық ықтимал примитивті көпмүшелердің саны {, мұнда Phi - Эйлер функциясы. Мұндай көпмүшелікпен берілген Регистр максималды кезеңнің жылжу регистрі деп аталады (немесе жалған кездейсоқ тізбектің генераторы), ал генерацияланатын тізбектер - максималды кезеңнің тізбектерімен (немесе М-тізбектермен). Сызықтық күрделілігі

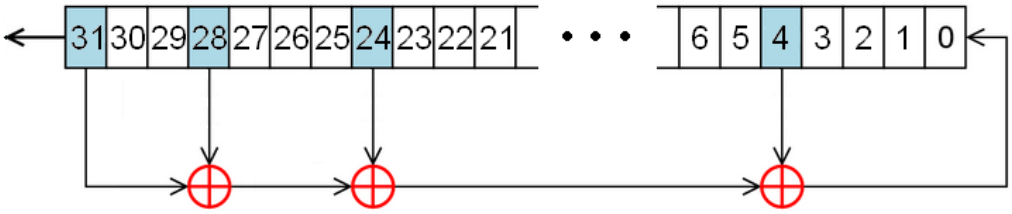
S=S0, S1, S2) шексіз екілік тізбектің сызықтық күрделілігі деп келесі түрде анықталатын L(S) саны аталады. егер S=(0,0,0,...)- нөлдік тізбек, онда L (S)=0; егер s генерациялайтын СКБЖР болмаса, онда L(S) = \infty; әйтпесе L(S) S жасайтын ең қысқа СКБЖР ұзындығына тең. Соңғы екілік тізбектің сызықтық күрделілігі-бұл тізбекті генерациялайтын ең қысқа СКБЖР ұзындығына тең сан.

Сызықтық күрделілігі тіркелімінің ығысу сызықтық кері байланысты көрсетеді, қаншалықты жақын генерируемая бірізділігі, қосымша, кездейсоқ. Соңғы екілік тізбектің сызықтық күрделілігін анықтаудың тиімді алгоритмі Берлекэмпа-Мэсси алгоритмі болып табылады.

2.3 Кері байланыспен жылжудың сызықтық регистрінің тіркеу реті

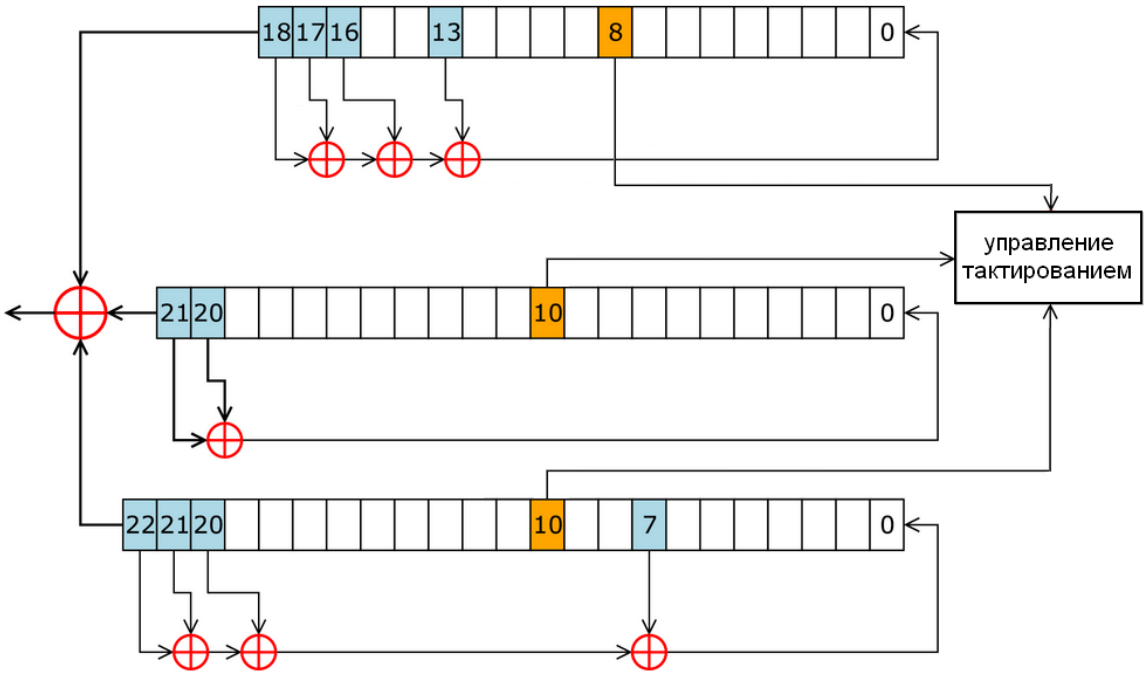
Кері байланыспен жылжудың сызықтық регистрі өзінен тіркеу (дәйектілігі бит берілген ұзындықтағы) және кері байланыстан тұрады. Әрбір тактіде келесі әрекеттер жүреді. Шеткі сол бит (үлкен бит) алынады, тізбек солға жылжиды және төмен түскен оң ұяшыққа (кіші бит) кері байланыс функциясының мәні жазылады. Бұл функция модуль бойынша тіркелімнің екі белгілі бір битін қосу болып табылады және дәрежесі бит нөмірін көрсететін көп нүкте түрінде жазылады. Алынған биттер шығу ретін қалыптастырады.

КБЖСР үшін негізгі көрсеткіш жалған кездейсоқ кезең болып табылады. Ол максималды болады (және 2^n-1 тең), егер кері байланыс функциясы 2 модулі бойынша қабылданса. Бұл жағдайда шығу тізбегі М-тізбектілік деп аталады[20].



2.3 Сурет – Сызықтық кері байланысы бар жылжу регистрі, $x^{32}+x^2+x^{25}+x^5+1$ кері байланыс көпжақты [9]

КБЖСР өзі криптоанализге оңай беріледі және шифрлауда пайдалану үшін жеткілікті сенімді емес. Практикалық қолдану әртүрлі ұзындықтармен және кері байланыс функцияларымен ауыспалы тактілеу регистрлерінің жүйесіне ие.



2.4 Сурет. A5/1 алгоритміндегі регистрлер жүйесі

A5 алгоритмінің құрылымы келесідей: Үш регистрде(R1, R2, R3) ұзындығы 19, 22 және 23 бит бар. кері байланысты көпмүшелер: $X^{19} + X^{18} + X^{17} + x^{14} + 1$ R1 үшін, $X^{22} + X^{21} + 1$ R2 үшін, $X^{23} + X^{22} + X^{21} + X^{8} + 1$ R3 үшін, тактілеуді басқару арнайы механизммен жүзеге асырылады.

- әрбір тіркелімде синхрондау биттері бар: 8 (R1), 10 (R2), 10 (R3),
- функция есептелінеді F = x&y|x&z|y&z, мұнда & — булево AND, | - булево OR, а x, y және z - синхрондау биттері R1, R2 және R3 сәйкесінше есептеледі,
- синхрондау биті F тең регистрлерді ғана жылжытады,
- шын мәнінде, синхробиті көпшілікке тиесілі регистрлер қозғалысы,
- Жүйенің шығыс биті- регистрлердің шығыс биттерінен XOR операциясының нәтижесі

2.4 СКБЖР шифрлауды бағдарламалық іске асыру әдісі

СКБЖР бағдарламалық жүзеге асыру жеткілікті баяу және егер олар Ассемблерде жазылса, тезірек жұмыс істейді. Шешімдердің бірі-16 СКБЖР параллельді пайдалану (немесе 32-к, компьютердің архитектурасындағы сөздің ұзындығына байланысты). Мұндай схемада көлемі жылжу регистрінің ұзындығына тең сөздер массиві қолданылады, ал әрбір бит сөздер өз СКБЖР жатады. Бұрылу тізбектерінің бірдей нөмірлері қолданылады, ол генератордың өнімділігіне елеулі ұтыстар бере алады. Фибоначчи *Конфигурациясы*

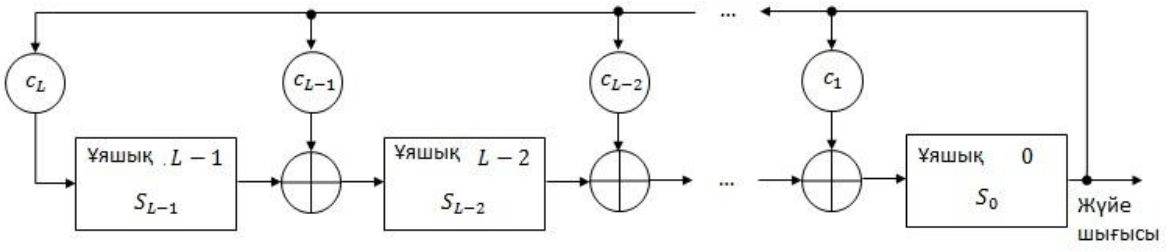
32-биттік жылжу регистрін қарастырайық. Ол үшін бұру тізбегі бар (32, 31, 30, 28, 26, 1). Бұл дегеніміз, жаңа битті генерациялау үшін XOR операциясының көмегімен 31-ші, 30-шы, 29-шы, 27-ші, 25-ші және 0-ші биттерді ойластыру қажет. Алынған СКБЖР -ның ең көп кезеңі $2^{32} - 1$. Si тілінде мұндай тіркелімге арналған Код келесі:

```
int LFSR_Fibonacci (void)
{
  static unsigned long S = 0x00000001;
  S = ((((S >> 31) ^ (S >> 30) ^ (S >> 29) ^ (S >> 27) ^ (S >> 25) ^ S ) &
0x00000001 ) << 31 ) | (S >> 1);
  return S & 0x00000001;
}
```

Галуа Конфигурациясы

Фибоначчи конфигурациясындағы сияқты кері байланыс схемасы генератордың шығуымен кіріс биттерінен XOR операциясының жиынтығы болып табылады, бірақ регистрдағы биттердің тәртібі кері: кіріс-L-1 бит, ал

Шығыс-0 бит болып табылады . Қосу нәтижесі келесі ұяшыққа жазылады, Ал Жаңа Шығыс бит L-1-ге жазылады. Сонымен, егер генерацияланатын бит нөлге тең болса, онда ұяшықтардағы барлық биттер өзгеріссіз оңға жылжиды, егер генерацияланатын бит бірлікке тең болса, онда бөлу биттері өзінің мәнін қарама-қарсы жаққа ауыстырады және барлық биттер оңға жылжытылады. Фибоначчи конфигурациясы және сол ұзындықтағы Галуа конфигурациясы бірдей, бірақ уақыт бойынша басқа жүйелерден ауысатын бір тізбекті жасайды (бұл ретте регистрлердің ішкі күйі өзгеше болуы мүмкін). Бұл генератор үлкен криптотөзімділікке ие емес, бірақ ол өнімділікке ұтысты береді: барлық XOR операцияларын параллельдеу арқылы жүзеге асыруға болады, Фибоначчи конфигурациясындағы сияқты бір бірінен кейін бірі емес. Бұл схема сондай-ақ аппараттық іске асыру кезінде ұтысты береді.



2.5 Сурет – Сызықтық кері байланысы бар жылжу Галуа регистрінің конфигурациясы

Ұзындығы 32 бит жылжу регистріне арналған код C тілінде былай сипатталады:

```
    {
  // for polynomial 0x80000057, reversed 0xea000001
  static unsigned long S = 0x00000001;
  if (S & 0x00000001) {
     S = ((S ^ 0xea000001) >> 1) | 0x80000000;
     return 1;}
  else {
     S >>= 1;
     return 0;}
}
```

.

Бұл функция LFSR_Galois функциясына қарағанда, Галуа конфигурациясындағы LFSR_ fibonacci функциясы шамамен 2 есе жылдам орындалады (Intel Core i5-те MS vs 2010 платформасында).

2.5 Годалардың генерациялануын бірізділік үлгісі

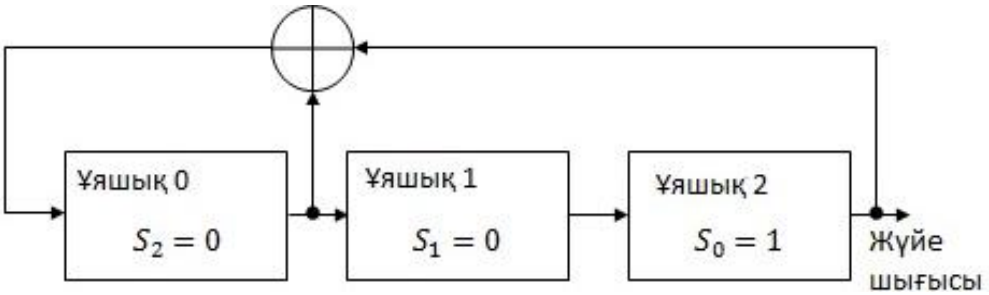
Фибоначчи Конфигурациясы. Фибоначчи конфигурациясының СКБЖР үлгісі СКБЖР $x^3 + x + 1$ сипаттамалық көпчленімен берілсін. Бұл дегеніміз, 2-ші және 0-ші, ал формуладағы бірлік 0-ші бит-кіріс дегенді білдіреді. Кері байланыс функциясы $S_j = S_{j-1} \oplus S_{j-3}$ түрі бар. Мысалы, жылжу тіркелімінің бастапқы жағдайы реттілік болды. Тіркелімнің кейінгі

Қадам нөмірі	Қалпы	Генерацияланатын бит
0	[0 0 1]	1
1	[1 0 1]	1
2	[1 1 1]	1
3	[1 1 0]	0
4	[0 1 1]	1
5	[1 0 0]	0
6	[0 1 0]	0
7	[0 0 1]	1

күйі төмендегі кестеде келтірілген:

2.1 Кесте – Ауысым регистрінің бастапқы күйі кезектілік болған кездегі

Жетінші қадамдағы ішкі жағдай бастапқы қадамға қайта оралғандықтан, келесі қадамнан бастап биттерді қайталайтын болады. Яғни, генерацияланатын тізбек мынадай:[1, 0, 0, 1, 1, 1, 0, 1 ….] (бит тәртібі СКБЖР генерациялау тәртібіне сәйкес келеді). Осылайша, бірізділік кезеңі 7-ге тең, яғни берілген көпмүшеліктің примитивтілігіне байланысты орын алған максималды мүмкін болатын мәнге тең. Бір ізді тіркеу күйлері төмендегі кестеде көрсетілген.



2.6 Сурет – СКБЖР Фибоначчи конфигурациясы

Жетінші қадамдағы ішкі жағдай бастапқы қадамға қайта оралғандықтан, келесі қадамнан бастап биттерді қайталайтын болады. Яғни, генерацияланатын тізбек мынадай: (бит тәртібі рслос оларды генерациялау тәртібіне сәйкес келеді). Осылайша, бірізділік кезеңі 7-ге тең, яғни берілген көпмүшеліктің примитивтілігіне байланысты орын алған максималды мүмкін болатын мәнге тең.

Сол сипаттамалық көп мағыналы алайық, яғни C_3=C_1=1, C_2=0. Шығу битімен тек 1 бит ғана қалыптасады. Бастапқы жағдайы бірдей. Тіркелімнің кейінгі күйі:

Жетінші қадамда тіркелімнің ішкі жағдайы бастапқы кезеңге оралды, демек, оның кезеңі де 7-ге тең. Фибоначчи конфигурациясына қарағанда, регистрдің ішкі күйі басқа болды, бірақ генерацияланатын бірізділік бірдей, тек 4 тактіге жылжыды (бит реті олардың СКБЖР генерациялау тәртібіне сәйкес келеді).

2.6 Қарапайым көпмүшеліктер генерациясы

СКБЖР көп мүшелілікті анықтауда шексіз өрістің бір элементінің әртүрлі дәрежелері сәйкес келе алатындығына қарамастан, көпмүшелерді формальды көбейтуге мүмкіндік береді. Шексіз өрістегі кез-келген функцияны бірнеше көпмүшеліктің көмегімен анықтауға болады (Лагранж интерполяциясы көпмүшесі)[26].

Көп мүшеліктерды мына фурмоламен анықталады. Көпмүшелік $f(x)$ - соңғы өріс үстінде F_q дың формальды қосындысы

$$f(x) = f_0 + f_1 x + \cdots + f_m x^m, \quad f_i \in F_q, f_m \neq 0 \qquad (2.4)$$

Мұнда m - көпмүшенің дәрежесі деп аталатын теріс емес бүтін сан $f(x), ax^k, k \in N_0$ ережеге сәйкес көбейту берілген алгебраның элементтері: $x^k \cdot x^m = x^{k+m}$, $x^0 = 1$

Примитивті көпмүшеліктің k дәрежесін генерациялау үшін $2^K - 1$ сандар көбейткіштерін білу керек . Көпмүшелерді кездейсоқ таңдау және оны примитивтілікке тексеру оңай. Тағы бір әдіс дайын кестелерді қолдану болып табылады, онда генератордың максималды кезеңін қамтамасыз ететін бұру тізбектерінің нөмірлері келтірілген. Ұзындығы 19 битке дейінгі максималды кезеңнің жылжу регистрлері үшін өрістің үстінде қарапайым көп жиіліктің кестесі келтірілген. Кез-келген берілген ұзындықтағы генераторда олардың қасиеттеріне сәйкес бір примитивті көпмүшелерден артық болуы мүмкін екенін ескеру қажет.

Осы заңдылқтар бойынша есептеуді жеңлдету үшін төмендегі кестені көпмүшеліктерді табуда пайдаланамыз

2.2 Кесте – Көпмүшеліктерді табу кестесі

Биттер	Қарапайым көпмүшелік	$2^K - 1$Период	Қарапайым полиномдар саны
2	$x^2 + x + 1$	3	1
3	$x^3 + x^2 + 1$	7	2
4	$x^4 + x^3 + 1$	15	2
5	$x^5 + x^3 + 1$	31	6
6	$x^6 + x^5 + 1$	63	6
7	$x^7 + x^6 + 1$	127	18
8	$x^8 + x^6 + x^5 + x^4 + 1$	255	16
9	$x^9 + x^5 + 1$	511	48
10	$x^{10} + x^7 + 1$	1023	60
11	$x^{11} + x^9 + 1$	2047	176
12	$x^{12} + x^{11} + x^{10} + x^4 + 1$	4095	144
13	$x^{13} + x^{12} + x^{11} + x^8 + 1$	8191	630
14	$x^{14} + x^{13} + x^{12} + x^2 + 1$	16383	756
15	$x^{15} + x^{14} + 1$	32767	1800

16	$x^{15}+x^{14}+x^{13}+x^{11}+1$	65535	2048
2.2 кесте жалғасы			
17	$x^{17}+x^{14}+1$	131071	7710
18	$x^{18}+x^{11}+1$	262143	7776
19	$x^{19}+x^{18}+x^{17}+x^{14}+1$	524287	27594

2.7 Құрылған шифрлық тізбектің криптографиялық тұрақтылығын арттыру жолдары

Көп ауысымды генераторлар құру. Генератордың бұл түрі сәйкесінше $x_{1,i}, x_{2,i} \ldots, x_{M,i}$, битін құрайтын кері байланыс ауыспалы бірнеше тізбегінен тұрады. Әрі қарай, шығарылған биттер булев $f(x_{1,i}, x_{2,i}, \ldots x_{M,i},)$ функциясымен өзгертіледі. Айта кету керек, осы типтегі генераторлар үшін $L_{i,} i = 1,2, \ldots, M$ регистрлерінің ұзындығы тұрақты. Генаратордың периотық кезеңін анықтау теңдеуі төменде көрсетілгендей.

$$T = (2^{L_1} - 1).(2^{L_2} - 1) \ldots ((2^{L_M} - 1) \leq 2^L \quad (2.5)$$

Ұяшықтардың жалпы саны.

$$L = \sum_{i=1}^{M} L_i \quad (2.6)$$

Демек, бірнеше СКБЖР пайдалану генератордың криптотөзімділігін арттырады бір тіркеліммен салыстырғанда генерацияланатын тізбектің кезеңін арттырады. Сондай-ақ, осы генераторға сәйкес келетін ең қысқа тіркелімнің сызықтық күрделілігі немесе ұзындығы артады. Мұндай регистр генерацияланатын бірізділік бойынша Берлекэмпа — Мэсси алгоритмінің көмегімен орналасқан. Ең жақсы жағдайда оның ұзындығы генерацияланатын кезектілік кезеңімен өлшенеді[4].

2.7 Сурет – Бірнеше жылжыту регистрі бар Генератор

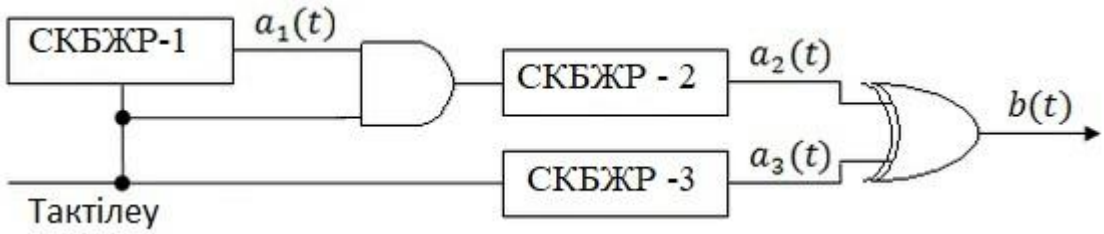
Сызықты емес түрлендіргіштері бар генераторлар**.** Мұндай генератордың құрылымдық сұлбасы алдыңғы генератордың схемасынан еш

айырмашылығы жоқ. Ең бастысы, түрлендіру құрылғысы сызықты емес $f(x_1, x_2, \ldots x_M)$булевой функциясымен берілген. Мұндай функция ретінде, мысалы, Полин Жегалкин алынады (Жегалкин теоремасына сәйкес, барлық булев функциясы жалғыз Полин Жегалкин болуы мүмкін).

Бейсызық генератор болуы мүмкін, сондай-ақ іске асырылды тіркелімінде ығысу сызықты емес кері байланыспен. Ол СКБЖР қарағанда көп максималды кезең $2^{2^{L-1}-1}$ тізбектерінің нұсқаларын бере алады[27].

Бұл генератордың криптотөзімділігі қолданылатын функцияның сызықсыз болуы есебінен жоғарылайды. Жалпы анықтау бойынша тіркелімдерді генератциялауы күрделі математикалық реттік бит болып табылады, өйткені белгілі алгоритмі қалыптастыратын бастапқы жағыдай.

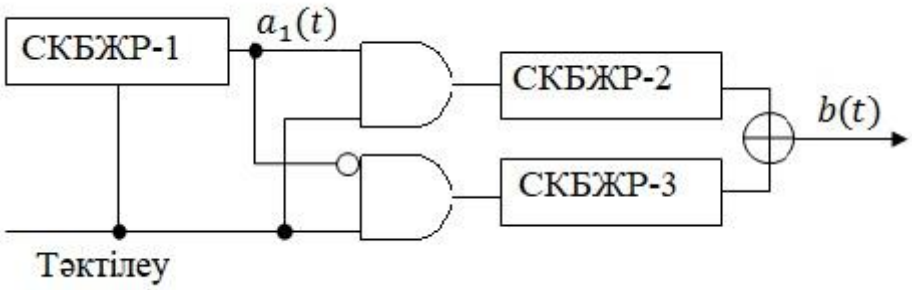
Бұл әдіс, мысалы, Гефа генераторында және гефа жалпыланған генераторында қолданылады.



2.8 Сурет – «тоқта-қетті» генераторы

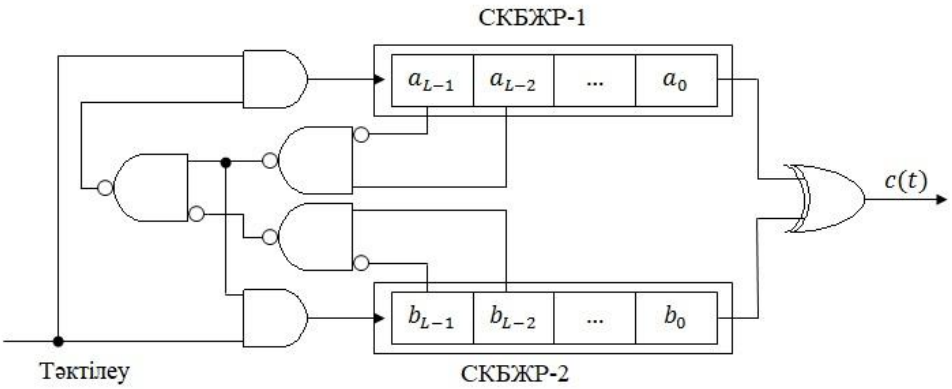
«тоқта-кетті» генераторы (ағылшынша Stop-and-Go, Both-Piper) 2.8-сурете тактілік жиілігін басқару үшін СКБЖР-1 шешімін қолданады, сондықтан СКБЖР-2 уақыт t_i сәтінде СКБЖР-1 шығымы бір бірлікке тең болса ғана өз күйін t_{i-1} уақытта өзгертеді. Бұл схема корреляциялық аутопсияға қарсы тұра алмады [28].

Криптотөзімділікті арттыру мақсатында ауыспалы «тоқта-кетті» генераторы ұсынылды. Онда әртүрлі ұзындықтағы үш жылжу регистрі қолданылады. Бұл жерде СКБЖР-1, 2-ші және 3-ші регистрлердің тактикалық жиілігін басқарады, яғни СКБЖР-2 СКБЖР-1 шығыспен бірлікке тең, ал СКБЖР-3, СКБЖР-1 шығымы нөлге тең болған кезде өз жағдайын өзгертеді. Генератордың шығуы СКБЖР-2 және СКБЖР-3 екі Шығыс модулі бойынша қосу операциясы болып табылады. Бұл генераторда үлкен периодтық және үлкен сызықтық күрделілігі бар. СКБЖР-1 корреляциялық ашу тәсілі бар, бірақ бұл генератордың криптографиялық қасиеттерін әлсіретпейді.



2.9 Сурет – Ауыспалы «тоқта-кетті» генераторы

Тактирлеудің күрделенген екі жақты «тоқта-кетті» генераторы қолданылған, онда бірдей ұзындықтағы жылжудың 2 регистрі қолданылады. Егер СКБЖР-1 t_{i-1} шығуы уақыттың кейбір сәтінде нөлге тең болса, ал уақыт кезінде - бірлікке тең болса, онда СКБЖР-2 t_{i-2} уақыт кезінде тактацияланбайды . Егер СКБЖР -2 шығымы t_i уақыт сәтінде нөлге тең болса, ал t_{i-1} уақыт сәтінде - бірлікке тең болса және егер бұл регистр t_{i-2} уақыт сәтінде тактацияланса, онда сол t_i сәтте СКБЖР-1 тактацияланбайды. Бұл схеманың сызықтық күрделілігі шамамен генерацияланатын тізбектің кезеңіне тең.



2.10 Сурет – Екіжақты «тоқта-кетті» генераторы

Желілік кері байланыспен жылжу регистрлері ағындық шифрларға (әсіресе әскери криптографияда) арналған жалған кездейсоқ тізбектегі генераторлар ретінде бұрын қолданылады. Дегенмен, СКБЖР сызықтық схема болып табылады және кейбір жағдайларда оңай сынуы мүмкін. Мысалы, криптоаналитик шифрланған мәтіннің бір бөлігін ұстап алады және ол бойынша жоғарыда аталған Берлекэмпа алгоритмі - Мэсси бастапқы СКБЖР имитациялайтын ең аз өлшемдегі СКБЖР қалпына келтіруі мүмкін. Содан кейін, ұстап алынған мәтін алынған тіркелімге берілуі және шифрленуі мүмкін. СКБЖР -қа негізделген ағын шифрларының криптотөзімділігін арттыру әдістері жоғарыда келтірілген.

Мына тіркелімінде ығысу сызықтық кері байланыспен негізделген мұндай ағынды шифрлар ретінде A5/1 A5/2, пайдаланылатын GSM стандартында шифры E0 қолданылатын Bluetooth. A5/2 шифры бұзылды, ал A5/1 және E0 шифрларының елеулі кемшіліктері бар. Сызықтық кері байланысымен жылжу регистрі сызықтық конкруэнтті генератормен тығыз байланысты.

3 Сызықтық кері байланысы бар жылжу регистрынның криптографикалық алгоритімін Matlab Simulink ортасында модельдеу

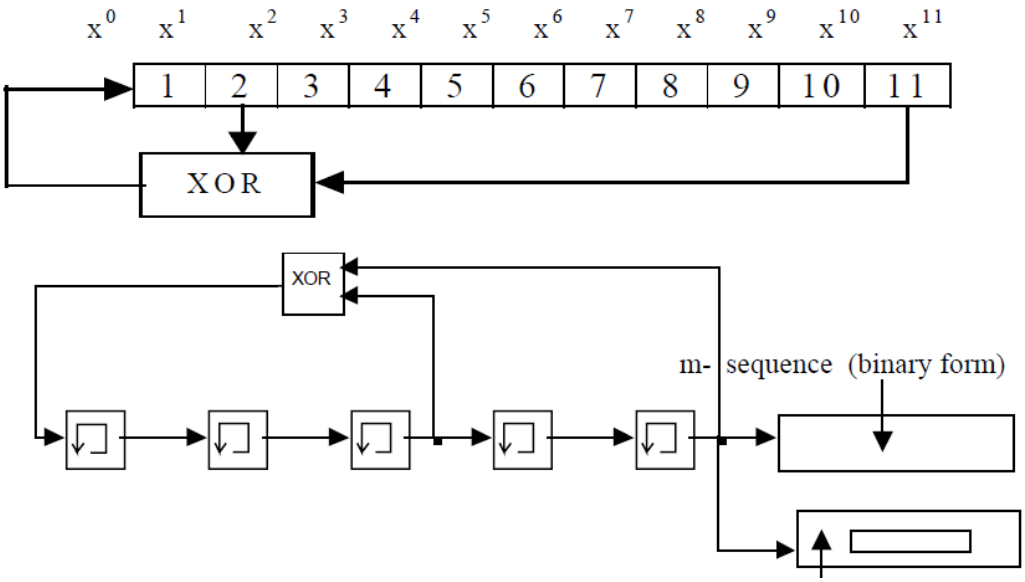
3.1 Шифрлық m тізбізбегін құру

Инженерия мен ғылымның көптеген салаларында үлкен маңызға ие. Бұл дипломдық жұмыста қосымшалардың ішіндегі ең көрнектісі ұялы байланыстағы ақпаратық криптографияны құруда қолданылатын сызықтық кері байланысы бар жылжу регистрінің жұмысын Matlab Simulink ортасында моделдеу.

Кездейсоқтық идеясы кезектіліктің келесі битін болжау мүмкін еместігін көрсетеді. Егер GF $(2^n - 1)$ ақырлы өрісінен алынған реттілік барлық $S_{i\in N} = S_1, S_2, \dots S_1$, мәндер аймағына сәйкес келмесе, онда ол жалған кездейсоқ немесе жалған-шу (ЖШ) тізбегі деп аталады. Сондықтан СКБЖР тізбектер - бұл белгілі қасиеттерге жауап беретін және оны құратын реттіліктер бар тізбек болып табылады.

СКБЖР көбінесе аппараттық дизайн арқылы жүзеге асырылады және ағындық шифрлар мен басқа қосымшалардың көмегімен жүгезе асырылады. СКБЖР-де биттер жады ұяшықтарының тізбегінде сақталады, онда сағат импульсі биттерді келесі кейінгі жад ұяшықтарына бағыттайды. Ұяшықтардың белгілі бір позициясының XOR әдісі әр сағат сайынғы импульстер үшін жаңа битті алу үшін қолданылады, бұл жағдайда соңғы ұяшық үнемі XOR процесінде қолданылады. Егер бастапқы жады ұяшықтарының әрқайсысына 0с жүктелмеген болса (бастапқы жағдай), шығарылған тізбектілік бірнеше кезеңнен тұрады. Шығарылған тізбекті максималды периодтығы $T = 2^N - 1$ арқылы циклдеуге болады, мұндағы n СКБЖР қолданылатын жад ұяшықтарының саны. Бұл дәйектіліктің максималды кезеңділігіне тек СКБЖР жад ұяшықтарының бірнеше нақты позицияларының кейбір комбинацияларын тек XOR енгізу арқылы қол жеткізуге болады. 3.1-суретте көрсетілген диаграммада 11 жад ұяшықтарынан тұратын СКБЖР бейнеленген, мұнда 2-ші және 11-ші жад ұяшықтарының қосындысы әр сағат импульсіндегі тізбектік қатардағы жаңа биттерді шығару үшін XOR- да өңделген. 1-суреттегі СКБЖР -нің осы нақты құрылымымен шығарылған дәйектілік 2047 кезеңділікке ие.

Полиномиялық формадағы XOR-позициясымен сипатталған СКБЖР құрылымы LFSR-ге тән полином деп аталады. Мысалы, 3.1-суреттегі криптологиялық сигналды құру алгоритімі. Мұнда СКБЖР жүйесі бар құрылымды көпмүшелік сипатталады.



3.1 Сурет – MATLAB - SIMULINK қолдана отырып (1+ x^3+ x^5) көпмәнді 5 биттік СКБЖР енгізу.

Максималды кезеңділік тізбегін ($T = 2^N - 1$) құратын СКБЖР жады ұяшықтарына негізделген құрылымның полиномиясы қарапайым полином деп аталады.

Егер СКБЖР шығарған жүйенің максималды кезеңділігі болса ($T = 2^N - 1$) онда бұл реттілік m-тізбегі деп аталады.

$C_3(x) = 1 + x^2 + x^3$ сипатталған көпмүшелікпен 3-биттік СКБЖР қарастырайық. Бастапқы жүктемелердің бәрі 1-ге тең. Содан кейін осы СКБЖР 2^3-1 бойынша алынған реттілік ұзынды 0100111 болады. Осылайша құрылған реттілік m-тізбектілік болып табылады, ал $C_3(x) = 1 + x^2 + x^3$ қарапайым көпмүшеліг.

Кездейсоқтықтың сандық өлшемін қамтамасыз ету үшін m-дәйектілігі бойынша статистикалық сынақтарды жүргізуге болады. Олар 0 және 1 сандарының белгілі бір заңдылықтарын салыстырмалы жиіліктерін S_i ретімен өлшейді.

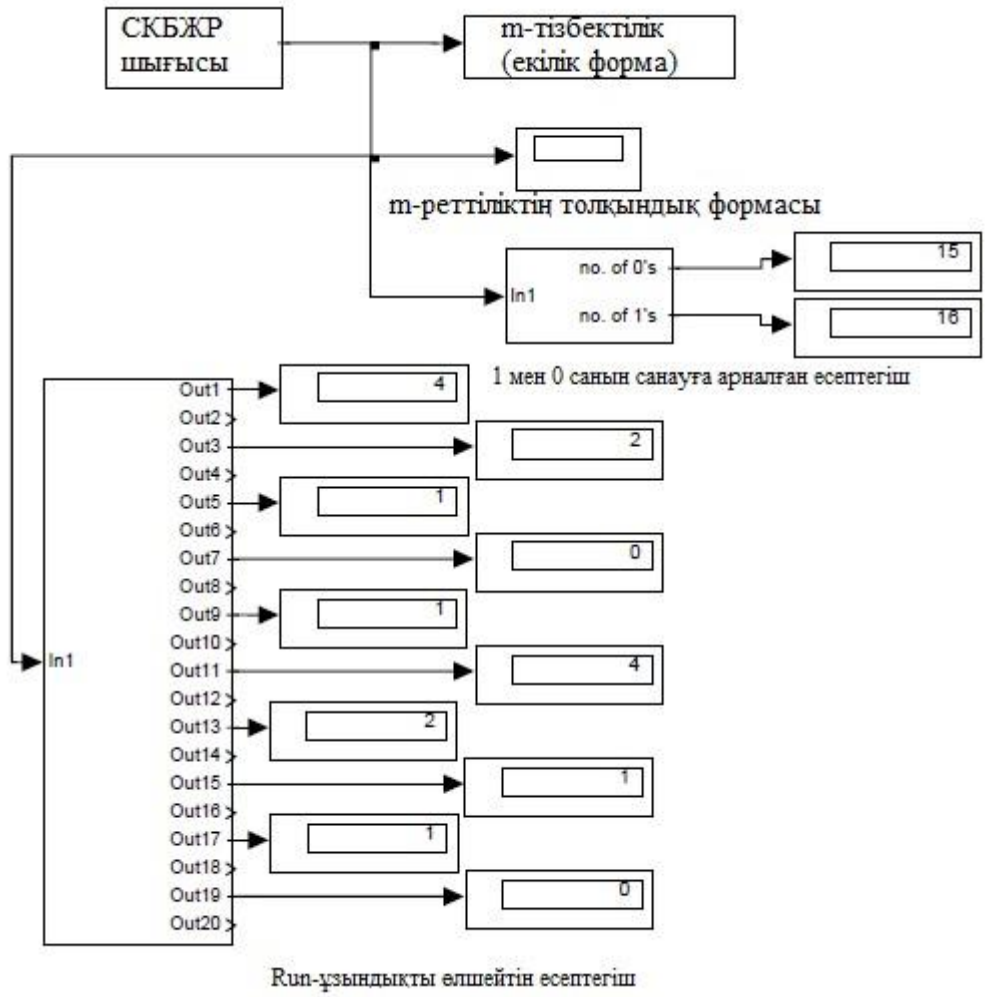
N-биттік СКБЖР шығарған m-реттіліктің әр кезеңінде 1-дің жалпы саны -ке 2^{N-1}тең болады. N-биттік СКБЖР жасаған m-дәйектіліктің әр кезеңінде 0-дің жалпы саны 1-ден кем болады, яғни 0-дің саны 2^{N-1}-1-ге тең болады. N-биттік СКБЖР жасаған m-дәйектілік кезеңі қатарынан 1-ге тең болады. N-биттік СКБЖР жасаған m-дәйектілік (n-1) периодында 1-дің кезектесуі болмайды. N-биттік СКБЖР тудыратын m-дәйектілік кезеңі кездейсоқ 0 ден тұрады. Run термині жалпы жағдайда бір класты элементтердің реттік тізбегін анықтауы мүмкін.

М-кезеңділік кезеңінде-1s және 0s топтарының тізбектелген тепе-теңдіктерін бөлу ($1 \le ч \le N - 1$ үшін орындалады) келесі теорема түрінде ұсынылған ережемен реттеледі.

m кезеңділіктегі T периотта СКБЖР арқылы N-битт құрылады, 0с сондайақ 1с кезінде (n-x-1) ден $1 \leq x \leq n-2$ ішінде 2^{x-1} бойынша қалыптастрады.

3.1 Кесте: Run 1 мен 0-дің жалпы санын есептейді

Run жилігі	1	0	0	1	1	1	2	2	4	4	Жалпы 1s	Жалпы 0s
1s және 0s топтарың байланысы	5 1s	5 0s	4 1s	4 0s	3 1s	3 0s	2 1s	2 0s	1 1s	1 0s	16	15



3.2 Сурет – SIMULINK- MATLAB ортасындағы криптографиялық шифрлау алгоритім моделі.

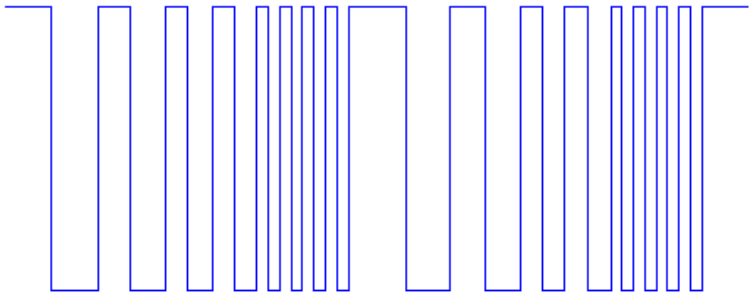
Барлық есептеуіштер қажетті іске қосу санын тексеру үшін сметериялы криптологиялық алгоритмдер негізінде модельделеді. Әзірленген жинақ 3.3-кестеде көрсетілгендей, екінші есептеуіштің шығыс деректерін оқиды.

3.3 Кесте – Екінші есептегішті шығару

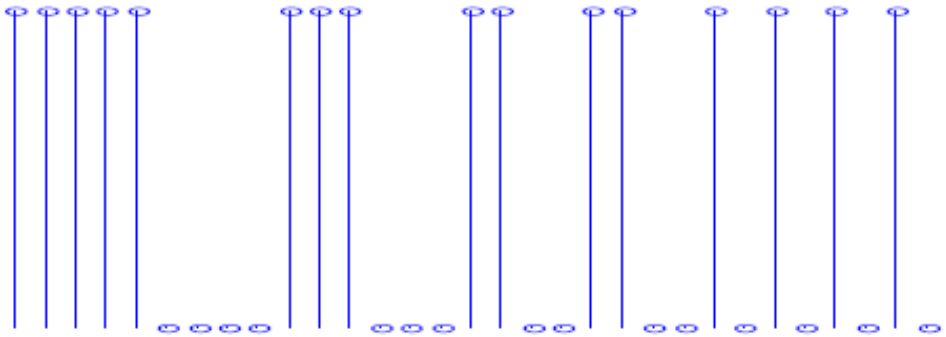
Шығу нөмірі (Функция)	Шығу нөмірі (Функция)
OUT1 - runs of 1 – 1s;	OUT11 - runs of 1 – 0s;
OUT3 - runs of 2 – 1s;	OUT13 - runs of 2 – 0s;
OUT5 - runs of 3 – 1s;	OUT15 - runs of 3 – 0s;

OUT7 - runs of 4 – 1s;	OUT17 - runs of 4 – 0s;
OUT9 - runs of 5 – 1s;	OUT19 - runs of 5 – 0s;

2-суретте SIMULINK - MATLAB көмегімен модельдендірілген СКБЖР көрсетілген, полиномдық дәрежесі n=5, көпмүшеліктің $(1 + x^3 + x^5)$ сипаттамасы бастапқы жағдайға ие (11111) және 31 $(2^5 - 1)$ кезеңі бар m-тізбегін s ті құрады. Екілік формадағы m-тізбектің шығыс файлы (11111000110111010100000100101100) ал осциллографтың толқындық формасы 3.1-суретте көрсетілген.



3.3 Сурет- түзілген m-тізбегінің үздіксіз толқын пішіні.



3.4 Сурет - Түзілген m-тізбегінің дискретті толқын пішіні.

3.2 М кезеңділіктің қасиеті - импульстік генератор ретінде жұмыс істеу

М-кезеңділік әр түрлі жиіліктегі импульстарды тудырады. Зерттеу әр түрлі импульстардың ені мен жиілігінің басқалармен нақты байланысы бар екенін көрсетеді (3.1-суретті қараңыз). 3-кестеде СКБЖР сағат импульсінің Т уақыт кезеңі бар екендігі ескеріліп, m-кезеңділігінің периоты үшін $(2^n - 1)$ бұл қасиет сипатталған.

3.2 Кесте – m-тізбегінде пайда болатын импульстар

Импульстар саны	1	1	$1 \le x \le n-2$ үшін 2^{x-1}	$1 \le x \le n-2$ үшін 2^{x-1}
Импульстің ені	nT	(n-1)T	(n-x-1)T	(n-x-1)T

Импульстің түрі	Белсенді жоғары	Белсенді төмен	Белсенді жоғары	Белсенді төмен

3.3 М-тізбектің авто-корреляциясы қасиеті

М-тізбегінің статистикасын және сипаттамасын зерттеу үшін оларды корреляциялық функциялары арқылы талдау қажет. Екі тізбектің корреляциялық функциясын олардың бір-бірімен қаншалықты сәйкес келетінін көру арқылы сипаттауға болады. Әр түрлі параметрлер тізбектің ұзындығын, тізбектер арасындағы фаза және СКБЖР тактілік жиілігі, екі тізбектің корреляциясына әсер етеді. Сигналдың корреляция актісі оның барлық вариациялары арқылы автокорреляция ретінде белгілі. Ac(k) автокорреляциялық функциясы м-кезектілік, мұндағы $((S_{i\epsilon N}) = S_1, S_2, \dots S_i \dots)$ ол $2^{N-1}, N = 1$ құралы оның k-жылжыту үшін берілуі мүмкін:

$$AC(k) = \frac{1}{N}\sum_{i=1}^{N} S_i S_{i+k}; 0 \leq k \leq N-1 \qquad (3.1)$$

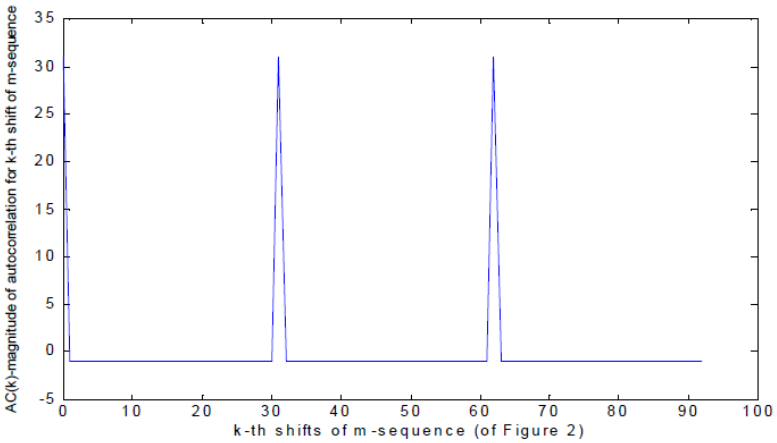
Мұндағы S_i - i-ші мәні - m-тізбегінің орны

М-тізбектің автокорреляциялық функциясы нөлдік ауысулар кезінде максимум 2^{N-1}-ге жетеді. Басқа ауысулар үшін ($1 \leq x \leq n-2$) оның мәні – 1-ге тең болады.

Simulink - MATLAB нұсқасының ортасындағы әзірленген жиынтық екі жеке есептеуіштен тұрады, олардың біреуі 1s және 0s қосынды сандарды есептеуді бақылайды. Тест-комплект моделінде екі қорек көз қарастырылған. Олар осциллограммаларды автокорреляциялық функцияны және М-реттілігін қамтамасыз етуге арналған. Сонымен қатар, m-бірізділіктің екілік нысанын жүктеу мүмкіндігі қарастырылған.

Біз MATLAB-SIMULINK моделін суретінде қалыптасқан дәйектілікті қолданамыз, 1 және 0 сандарының санын, сондай-ақ Run ұзындығын санауға болады (3.3-кестеге сәйкес).

Осы толқын формасын зерттеу импульстік қасиеттердің 3.2-кестеде көрсетілген ережелерге сәйкес келетіндігін анықтайды. Басқа аймақтың шығуы 3.2-суретте көрсетілген. Оны 3.2-сурет арқылы автокорреляцияның шыңы AC(k) арқылы көруге болады. 3.1-теңдеуі нөлдік ығысу кезінде 31-ге тең, құрылған m-тізбектің әр циклінде қайталанатындығын көруге болады. нәтиже 3.1-теңдеуде келтірілген m-тізбектің автокорреляциялық қасиетін қанағаттандырады.



3.5 Сурет – m-тізбектің автокорреляциялық қасиеті.

Осылайша, криптографиялық сметериялы шифрлау кезінде СКБЖР-да m-дәйектер теориясын пайдаланып құруға болатынана көзжеткіздік. Атап айтқанда 1-кестеде берілген зерттеу m-дәйектіліктің қаншалықты маңызды екенін көрсетеді. Біз қарапайым мобилді байланыс саласындағы криптографиялық сметериялы шифрлау құруға болатынына көз жеткіздік. Қауіпсіздік ақпараттық технологиялар заманымыздаға өмірлік маңызды мәселе болғандықтан, ақпаратың жағалуына, ұрлануына жол бермеу үшін осы қарапай алгоритім құруды біліумізкерек. Бұндай шифрлауды Intel® архитектурасындағы топтамалармен іске асыруға болад.

ҚОРТЫНДЫ

Дипломдық жұмыста криптографиялық алгоритмдердің тұрлері мен негізгі әдістеріне қысқаша шолу жасалды. Сонымен қатар телекомуникаця жүйесінде GSM ұялы стандартына криптографиялық алгоритмдерін енгізу бағытарына талдаулар жасалды. СКБЖР негізінде құрылған криптографиялық алгоритмды ұялы байланыс жүйесінде қолдану технологиясына талдау жасап, криптотөзімділікті арттыру мақсатында ауыспалы «тоқта-кетті» генераторына әртүрлі ұзындықтағы үш жылжу регистрін қолдануды қарастрдық.

Ұялы байланыс жүйесінде СКБЖР негізінде құрылған криптографиялық алгоритмды MATLAB.SIMULINK-ортасында моделденді. М-тізбегінің статистикасын және сипаттамасын зерттеу үшін әр түрлі параметрлер тізбектің ұзындығын, тізбектер арасындағы фаза және СКБЖР тактілік жиілігі т.б. екі тізбектің корреляциясы салыстырылып нәтиже алынды.

Артықшылықтары. СКБЖР негізінде құрылған криптографиялық алгоритмдердің жоғары жылдамдығы. Барлық есептеуіш құрылғыларда аппараттық түрде іске асырылған қарапайым биттік операцияларды қосу және көбейту ғана қолдану. Жақсы криптографиялық қасиеттері бар (СКБЖР жақсы статистикалық қасиеттері бар үлкен кезеңнің кезектілігін тудыруы мүмкін). Өз құрылымының арқасында СКБЖР алгебралық әдістерді қолдана отырып оңай талданады.

Кемшіліктер. СКБЖР-тың басты проблемаларының бірі, олардың бағдарламалық іске асырылуы өте тиімсіз: кері байланыстың сиретілген көп нүктелерін болдырмау керек, өйткені олар корреляциялық ашумен бұзуды жеңілдетуге алып келеді, ал тығыз көп нүктелер өте баяу есептеледі. Сондықтан мұндай генератордың бағдарламалық іске асырылуы DES-ты іске асыруға қарағанда жылдамырақ жұмыс істейді.

ПАЙДАЛАНҒАН ӘДЕБИЕТТЕР

1. Shannon C.E. Communication Theory of Secrecy Systems. Bell Systems Technical Journal 28, 1949, p. 656 – 715.
2. Federal Information Processing Standards Publication 46-2. Data Encryption Standard (DES). NIST, US Department of Commerce, Washington D.C, 1993.
3. Криптографическая защита информации в АСУ СН. Курс лекций. В.И. Долгов. ХВУ. 2006.
4. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ. 2002.
5. Брюс Шнайер. Прикладная криптография. 2-ое издание. Протоколы, алгоритмы и исходные тексты на языке С. Доступно: http://nrjetix.com/r-and-d/lectures.
6. Raj Pandya, “Mobile and Personal Communication Systems and Service”s, 2001 IEEE PRESS, New York.
7. Dr. Kamilo Feher, “Wireless Digital Communication – Modulation and Spread Spectrum Applications, 2000” Prentice Hall of IndiaPrivate Ltd., New Delhi.
8. William Stallings, “Cryptography and Network Security”, 1991 Pearsen Education, New York.
9. C E Veni Madhavan & P K Saxena, “Recent Trends in Applied Cryptology”, IETE Technical Review, Vol 20, No 2, March-April 2013.
10. Marc Briceno, Ian Goldberg and David Wagner, “A Pedagogical Implementation of the A5/1, 2009.
11. Eli Biham and Orr Dunkelmna, “Cryptanalysis of the A5/1GSM stream Cipher”, 2010.Ross Anderson, Mike Roe, “A5-The GSM Encryption Algorithm”,2012.
12. Stefan Pitz, Roland Schmitz, Tobias Martin, “Security mechanism in UMTS”, Datenschutz and Datensicherheit (DUD), vol 25, pp 1-10, 2001.
13. Li Wei Dai Zibin Nan Longmei, “ Research and Implementation of High speed Reconfigurable A5 Algorithm”,2008 IEEE.
14. Fayyaz Ahmed, Dr. Mudassar Imran, “ Cryptographic Analysis of GSM Network”, 2017 IEEE.
15. Musheer Ahmad and Izharuddin “ Enhanced A5/1 Cipher with improved linear Complexity” 2018 IEEE
16. S.R. Masadeh, S. Aljawarneh, N. Turab, and A. M. Abuerrub, "A comparison of data encryption algorithms with the proposed algorithm: Wireless security," Sixth International Conference on Networked Computing and Advanced Information Management, 2010, pp. 341-345.
17. D.S.A. Elminaam, H. M. Abdual-Kader, and M.M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," International Journal of Network Security, vol. 10, pp 216-222, 2010.

18. J.J. Amador and R.W. Green, "Symmetric-key block cipher for image and text cryptography," International Journal of Imaging Systems and Technology, vol. 15, pp. 178-188, 2005.
19. A. Ramesh and A. Suruliandi, "Performance analysis of encryption algorithms for Information Security," International Conference on Circuits, Power and Computing Technologies, 2013, pp. 840-844.
20. Geremia, Patrick. "Cyclic Redundancy Check Computation: An Implementation Using the TMS320C54x". Texas Instruments. p. 6. Retrieved October 16, 2016.
21. Press, William; Teukolsky, Saul; Vetterling, William; Flannery, Brian (2007). Numerical Recipes: The Art of Scientific Computing, Third Edition. Cambridge University Press. p. 386. ISBN 978-0-521-88407-5.
22. Klein, A. (2013). "Linear Feedback Shift Registers" . Stream Ciphers. London: Springer. pp. 17–18. doi:10.1007/978-1-4471-5079-4_2. ISBN 978-1-4471-5079-4.
23. A. Poorghanad, A. Sadr, A. Kashanipour" Generating High Quality Pseudo Random Number Using Evolutionary Methods", IEEE Congress on Computational Intelligence and Security, vol. 9, pp. 331-335 , May,2008.
24. Klein, A. "Linear Feedback Shift Registers" (PDF). Stream Ciphers. London: Springer. pp. 17–18. doi:10.1007/978-1-4471-5079-4_2. ISBN 978-1-4471-5079-4, (2013)..