ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

Кәріпжан Мағжан Айболұлы

«Ауыстыру блоктарының криптографиялық қасиеттері»

Дипломдық жоба

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В100200 – «Ақпараттық қаупсіздік жүйелері» мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____Н.А.Сейлова
«__14__» ____05____2019 ж.

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: «Ауыстыру блоктарының криптографиялық қасиеттері»

Мамандығы 5В100200-Ақпараттық қаупсіздік жүйелері

Орындаған Кәріпжан М. А.

Пікір беруші
«Қазтелепорт» АҚ
Басқарушы директор
_____Төлеулиев С.Б.
«__13__» ____қаңтар____ 2019 ж.

Ғылыми жетекші
Лектор
_____Ибраев Р.Б.
«__18__» ____қаңтар____2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

5В100200- Ақпараттық қаупсіздік жүйелері

БЕКІТЕМІН
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____Н.А.Сейлова
«_14_» _____05_____2019 ж.

Дипломдық жобаны орындауға
ТАПСЫРМА

Білім алушы *Кәріпжан Мағжан Айболұлы*
Тақырыбы: *«Ауыстыру блоктарының криптографиялық қасиеттері».*
Университет Ректорының *2018 жылғы «16» 10 №3252-II* бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *2019жылғы «28» 04*
Дипломдық жобаның бастапқы берілістері: *Ауыстыру блоктарының криптографиялық қасиеттерін зерттеу. Криптоталдауға төзімді ауыстыру блоктарын генерациялау..*
Дипломдық жобада қарастырылатын мәселелер тізімі
1. Теориялық ақпарат
2. Тәжірбиелік зерттеулер
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызба материалдары 13 слайдта көрсетілген
Ұсынылған негізгі әдебиет *12 атаудан тұрады*

Дипломдық жобаны дайындау

КЕСТЕСІ

Бөлім атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімі	Ескерту
Теориялық ақпарат	16.03.2019-26.03.2019	
Тәжірибелік жұмыс	07.04.2019-28.04.2019	

Дипломдық жобабөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жобаға қойған

қолтаңбалары

Бөлімдер атауы	**Кеңесшілер аты, әкесінің аты, тегі (ғылыми дәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Норма бақылау	Зиро А.А., техника ғылымдарының магистрі	13.05.2019	

Ғылыми жетекшісі Ибраев Р. Б.

Тапсырманы орындауға алған білім алушы Кәріпжан М. А.

Күні «13» мамыр 2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Кәріпжан Мағжан Айболұлы
(студенттің Т.А.Ә.)
5В100200 Ақпараттық қауіпсіздік жүйелері
(мамандықтың шифрі және атауы)
дипломдық жобасына
(жұмыс түрінің атауы)

Тақырыбы: Ауыстыру блоктарының криптографиялық қасиеттері.

Қазіргі заманда құпия ақпаратты сақтау, өңдеу, тасымалдау өзекті мәселердің бірі. Мемлекеттік стандарттар негізінде қорғалған, жасырын ақпаратты заңсыз қол жеткізуге жасалатын қадамдар іске асатын болса стандарттың өзектілігі жоғалады.

Яғни, шифрлау алгоритмдерінде ашық мәтін мен жабық мәтін арасындағы статистикалық байланысты, блоктық симметриялы шифрларда сызықсыз ауыстыру блоктары қамтамасыз етеді. Ауыстыру түйіндерін генерациялау барысында оның кездейсоқ болуы шифрдың криптотұрақтылығын арттырып, сызықты және дифференциялды шабуылдарға төтеп беруін арттырады.

Сондықтан, М.А. Кәріпжанның дипломдық жобасының тақырыбы блоктық симметриялы шифрларда қолданылатын ауыстыру блоктарының криптографиялық қасиеттерін зерттеп, криптоталдауға тұрақты ауыстыру түйіндерін генерациялап шығаруға байланысты.

М.А. Кәріпжан дипломдық жұмыста ауыстыру блоктарының криптографиялық қасиеттерін булевтік функциялардың қасиеттері ретінде көрсетіп, сол буль алгебрасының қасиеттерін зерттей келе криптоталдауға төзімді сызықсыз ауыстыру түйіндерін генерациялады.

Дипломдық жобаны толық көлемде іске асыру студенттің университетте оқу кезіндегі игерген теориялық білімдерінің деңгейін ғана көрсете қоймай, сонымен қатар берілген тапсырма бойынша тәжірибелік іс-шараларды жүзеге асыра алатындығын көрсетті.

Жұмыстның мақсаты, оған жетудің міндеттері мен мазмұны, сондай-ақ жасалған қорытындылары арасындағы логикалық байланыс бар. Жобаның тұтастығы жұмыстың негізгі бөлімдері арасындағы тығыз қарым-қатынастпен және берілген тақырыбы мен зерттеу объектілерінен алшақтаудың жоқтығымен сипатталады.

Дипломдық жобаны жазу кезінде М.А. Кәріпжан теориялық материалдарды жинақтау, оларды талдау бойынша жұмысты жүргізіп, білімі мен дағдыларын пайдалана отырып криптографиялық қасиеті жақсы ауыстыру блоктарын генерациялап шықты. Сонымен бірге ол мақсаткерлікті, дұрыс шешімдер жасауды көрсете алды. Автор жіберілген қателерді түзету бойынша жұмыс атқарды.

Жалпы алғанда, баяндалғандардың негізінде Кәріпжан Мағжан Айболұлының дипломдық жобасы аяқталған жұмыс болып табылады және қорғауға ұсынылуы мүмкін.

Ғылыми жетекші
лектор
(лауазымы, ғылыми дәрежесі, атағы)
(қолы) Ибраев Р.Б.

2019 жылғы «13» мамыр

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И.СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

Дипломдық жұмысқа
Кәріпжан Мағжан Айболұлы
5В100200- Ақпараттық қауіпсіздік жүйелері

Тақырыбы: «Ауыстыру блоктарының криптографиялық қасиеттері»

Орындалды:
a) графикалық бөлім____парақ
b) түсініктеме____бет

ЖҰМЫС ӨЗЕКТІЛІГІ

Бұл жұмыстың өзектілігі заманауи блоктық симметриялы шифрларда қолданылатын ауыстыру блоктарының крипторграфиялық қасиеттерін булевтік функция негізінде зерттеп, кең таралған шабуылдарға криптотұрақтылығы жоғары және жақсы криптографиялық қасиеттерге ие түйіндерді генерациялау.

ЖҰМЫСҚА ЕСКЕРТУ

Дипломдық жұмыс бойынша айтарлықтай кемшілік жоқ, тек грамматикалық қателер барын ескерсек, аталған кемшілік жүргізілген зерттеуге әсері жоқ.

ЖҰМЫСТЫҢ БАҒАСЫ

Жұмысты орындау деңгейі өзінің нақтылығымен және өзектілігімен «Ақпараттық қауіпсіздік» мамандығы бойынша бакалавр дәрежесі үшін орындалатын дипломдық жұмыстарға қойылатын талаптарға сай және жұмыспен таныса келе, сапасын 95 %-ға бағалауға болады.

Пікір беруші
«Қазтелепорт» АҚ
Басқарушы Директор
_____ Төлеулиев С.Б.
«__»_____2019 ж

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Кәріпжан Мағжан

Название: Ауыстыру блоктарының криптографиялық қасиеттері

Координатор: Ренат Ибраев

Коэффициент подобия 1:0,2

Коэффициент подобия 2:0

Тревога:1

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

 обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
 обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
 обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

.....
.....
.....
.....
.....

.....

Дата 14.05.192

.....

Подпись заведующего кафедрой /

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

.....
.....
..... Корнеуте допускается .....
.....
.....

....

Дата 14.05.19. *Подпись заведующего кафедрой /*

начальника структурного подразделения

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Кәріпжан Мағжан

Название: Ауыстыру блоктарының криптографиялық қасиеттері

Координатор:Ренат Ибраев

Коэффициент подобия 1:0,2

Коэффициент подобия 2:0

Тревога:1

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

работа выполнена самостоятельно,
допускается к защите

13.05.19г. Р. Сорраев

Дата *Подпись Научного руководителя*

АҢДАТПА

Бұл дипломдық жұмыста негізінен блоктық шифрларда қолданылатын сызықсыз түрлендіру S-блоктарының криптографиялық қасиеттеріне аса назар аударылады. Ауыстыру блоктарының крипторграфиялық қасиеттері векторлық булевтік функцияның қасиеттері негізінде түсіндіріледі. Булевтік функцияның, ашып айтқанда, жоғарғы алгебралық дәреже, теңестірілу және толықтай теңестірілу, лавинды сипаттамалары, сызықты құрылымның болмауы, корреляциялық иммундық, жоғарғы сызықсыздық, алгебралық иммундық сияқты негізгі криптографиялық қасиеттері сиппатталады. Ауыстыру блоктарын қолданатын AES, ГОСТ Р 34.12 – 2015, СТБ 34.101.31 – 2011 (BELT) стандарттарындағы ауыстыру блоктарының қасиеттері өзара салыстырылады. Векторлық булевтік функцияны құрылу әдістерін пайдаланып, қасиеті криптоталдауға төзімді ауыстыру блогын генерацияланады.

АННОТАЦИЯ

В этой дипломной работе особое внимание уделяется криптографическим свойствам S-блоков нелинейного преобразования, которые в основном используются в блочных-шифрах. Криптографические свойства S-блоков объясняются на основе свойств векторной булевой функции. Характеризуются основные криптографические свойства булевых функций, такие как, высокая алгебраическая степень, уравновешенность и совершенная уравновешенность, лавинные характеристики, корреляционная иммунность и устойчивость, высокая нелинейность, алгебраическая иммунность. Сравниваются свойства S-блоков стандартов, таких как AES, ГОСТ Р 34.12 – 2015 и СТБ 34.101.31 – 2011 (BELT). С помощью методов построения векторной булевой функции генерируются блоки нелинейного преобразования, свойство которых устойчиво к криптоанализу.

ANNOTATION

In this thesis, special attention is paid to the cryptographic properties of S-blocks of nonlinear transformation, which are mainly used in block ciphers. The cryptographic properties of S-boxes are explained based on the properties of a vectorial Boolean function. The basic cryptographic properties of Boolean functions are characterized, such as, a high algebraic degree, poise and perfect poise, avalanche characteristics, correlation immunity and stability, high nonlinearity, algebraic immunity. The properties of S-block standards are compared, such as the AES, GOST R 34.12 - 2015 and STB 34.101.31 - 2011 (BELT). Using methods for constructing a vector Boolean function, nonlinear transformation blocks are generated whose property is resistant to cryptanalysis.

МАЗМҰНЫ

КІРІСПЕ 7
1 Керекті анықтамалар мен белгілер 9
1.1 Блоктық шифрлар 10
1.2 SP-желісі 10
1.3 Фейстель желісі 11
1.4 Потоктық шифрлар 12
2 Актуалдылық 14
3 Векторлық булевтік функцияның криптографиялық қасиеттері, криптографиялық алгоритмдердің сенімділігіне әсері 15
3.1 Жоғары алгебралық дәреже 16
3.2 Теңестірілу 16
3.3 Толықтай теңестірілу 17
3.4 Лавиндық сипаттамалары 18
3.5 Корреляционндық иммунндық және тұрақтылық 19
3.6 Жоғары сызықсыздық 22
3.7 Алгебралық иммуннитет 24
4 AES, ГОСТ 34.12-2015, СТБ 34.101.31-2011 ауыстыру блоктарының криптографиялық қасиеттерін салыстырмалы талдау 28
5 Криптографиялық тұрақты векторлық булевтік функцияны генерациялау әдістері 34
6 Векторлық булевтік функцияны генерациялау және криптографиялық қасиеттерін зерттеу 37
ҚОРЫТЫНДЫ 41
ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ 42
Қосымша А 43
Қосымша Б 46

КІРІСПЕ

Ғаламтор заманында деректерді жасырын тыңдау мен заңсыз өзгертуден қорғау маңызды мәселердің біріне айналып отыр. Мұндай қорғаныс кілттерсіз оқу мүмкін емес ету үшін деректерді түрлендіретін шифрлар сияқты криптографиялық примитивтермен, кез келген ұзындықтағы кез келген екілік кодтарымен саусақ іздерін байланыстыратын хэш-функциялармен немесе хабардың өзгермегеніне кепілдік беру үшін пайдаланылатын хабарламаны аутентификациялау кодымен (MAC) қамтамасыз етіледі.

Осындай криптографиялық примитивтерді әзірлеу күрделі тапсырма, ол компьютерлердің өнертабысынан бастап таза математика мен информатиканың тоғысында белсенді талқыланды. Криптографиялық примитивтердің екі негізгі тобы бар: асимметриялық және симметриялық. Асимметриялық криптография шифрлау кілті ашық, құпия емес түрде болады да, ал шифрін кері ашуға қажетті кілт құпия түрде сақталынатын криптожүйелерді құрумен айналысады. Бірақ бізді шифрлау мен шифрін кері ашу үшін бірдей (құпия) кілт қолданатын симметриялық крипторграфия қызықтырады.

Симметриялық шифр жасау кезінде оны әзірлеушілер көптеген нәрселерге көңіл аударуы тиіс. Ол қарапайым дербес компьютерде, сондай-ақ әлдеқайда аз қуатты орнықтырылған жүйелерде жұмыс істеу кезінде жылдам болуы керек. Криптографтар оның сапасын бағалау үшін оны зерттеу мүмкіндіктерімен қатар белгілі бір құрылымды пайдаланған абзал. Нәтижесінде, бізге белгілісі, ол қорғалуы тиіс. Бірақ бұл жерде " қорғалған " дегеніміз не? Жақсы қауіпсіздігі бар шифр – бұл қаскүнемдердің шифрланған мәтінге сәйкес келетін ашық мәтінді қалпына келтіре алмайтындығы интуитивті түсінікті, атап айтқанда, кілтті қалпына келтіретін барлық практикалық мақсаттар үшін мүмкін емес болуы тиіс шифр. Бұл шифрларға қол жеткізу үшін әдетте араластыру мен шашыратуды (Шеннон конструкциясы) қамтамасыз ететін сызықтық операциялар мен сызықтық емес операциялардың көптеген комбинацияларынан тұрады. Сызықтық емес операциялар жиі F_{2^m}-нен F_{2^n}-ге дейін ауыстыру блогы немесе S-box деп аталатын ішкі функциялармен орындалады, мұнда F_{2^n}, 2^n өлшемінің соңғы өрісі.

Екілік тізбекті шифрлау үшін қолданылатын кілтті алуға мүмкіндік беретін әдіс шабуыл деп аталады. Шабуылдардың мысалы ретінде сызықтық шабуылдар мен алгебралық шабуылдар болып табылады. Шифрдың тұрақты болуының бір көрінісі дифференциалды шабуылдарға төзімділігі. 90-шы

жылдардың басында Бихам мен Шамир енгізген ерекше қасиеттері бар S-блоктардың көмегімен дифференциалды шабуылдарды алдын алынуы мүмкін болды.

Криптографиялық ақпаратты өңдеуде заманауи алгоритмдердің құрылуы сызықсыз ауыстыру блоктары мен сызықты шашыратуды қарапайым және жақсы зерттелген крипторграфиялық примитивтерге итеративті түрде қолдану көрініс табуда.

Сызықсыз ауыстыру блоктарын құруда жасалынатын негізгі қадам ретінде дамыған булевтік алгебраны қолдану, сызықсыз ауыстыру түйіндерін арнайы түрде таңдалған булевтік функциямен көрсетуге мүмкіндік береді. Яғни ауыстыру блоктарын булевтік функцияның композициясы ретінде көрсетіп, оның қасиеттерін зерттеу.

1 Керекті анықтамалар мен белгілер

n – натурал сан деген ұғымды енгіземіз; F_2 – 1 және 0-ден тұратын көпмүше; $x = (x_1, \dots, x_n) – F_2$ координаты бар екілік вектор; F_{2^n} – n ұзындықтағы барлық векторлардың жиынтығы; 0 = (0, … ,0) – нөлдік вектор; $\oplus$ - екілік модуль бойынша көбейту.

x екілік векторының *Хэмминг салмағы деп* $wt(x)$ – x-тің құрамындағы бірліктердің саны. *Хэмминг аралығы* $d(x, y)$ деп – екі x, y векторының арасындағы және олардың айырмашылығы бар позиция саны. Ол $d(x, y) = wt(x \oplus y)$-ке эквивалентті. (x, y) екілік векторының скалярлы көбейтіндісі, $(x,y) = x_1y_1 \oplus \dots \oplus x_ny_n$ өрнегі арқылы анықталады.

n-айнымалысының *булевтік функциясы* F_{2^n}-нің F_2-ге еркін кескінделуі. f булевтік функциясының $wt(f)$ салмағы оның мәндерінің векторындағы бірліктер санына тең. f және g булевтік функцияларының арасындағы $d(f,g)$ *Хэмминг аралығы* деп функциялардың мәндері әртүрлі болатын векторлардың саны.

F векторлық булевтік функциясы ((n, m) - функциясы) деп F: F_{2^n}-нің F_{2^m}-ге еркін кескінделуі. n айнымалысының F булевтік функциясы деп m = 1 болған жағдайда айтылады. m кординатты булевтік функцияны n айнымалысынан (n, m) – функциясының жиынтығы ретінде қарастырса болады: F = (f1, ... , f2). Компоненттік функция деп кординатты функцияның кез-келген нөлдік емес сызықты комбинациясы айтылады, сондай-ақ (b, F), мұндағы $b \in F_{2^m}$, $b \neq 0$ негізіндегі булевтік функция.

Кез-келген (n, m)-функцияны *Жегалкин полиномы* немесе *алгебралық нормалды формада (АНФ)* жазуға болады: $F(x_1, \dots, x_n) = \bigoplus_{k=0}^{n} \bigoplus_{i_1,\dots,i_k} a_{i_1,\dots,i_k} x_{i_1} \dots x_{i_k} \oplus a_0$, мұндағы $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ және $a_{i_1,\dots,i_k} \in F_{2^m}$.

F функциясының *deg(F) алгебралық дәрежесі деп* АНФ-тың ең ұзын қосынды айнымалы саны деп аталады. Сондай-ақ коэффициент нөлдік векторға тең емес. Дәрежесі 1-ден аспайтын функция, ал $a_0=0$ жағдайындағы функция *сызықты* деп аталады.

$W_f(y) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus (x,y)}$ теңдігімен анықталатын n айнымалысынан f-тің $W_f(y)$ булевтік функциясы әр $y \in F_{2^n}$ үшін *Уолш-Адамар коэффициенті* деп аталады. f булевтік функциясының *Уолш-Адамар спектрі* деп барлық $y \in F_{2^n}$ үшін $W_f(y)$-тің коэффициенттер жиынтығы аталады. *Персеваль теңдігін* $\sum_{x \in F_2^n} W_f^2(y) = 2^{2n}$ өрнегі қанағаттандырады. Векторлық функцияның Уолш-Адамар спектрі Уолш-Адамардың барлық коэффициенттерінен және оның

компонентті булевтік функциясынан тұрады: $W_F(u,v) = \sum_{x \in F_2^n} (-1)^{(v,F(x)) \oplus (u,x)}$.

1.1 Блоктық шифрлар

Блоктық шифр ашық мәтіннің (хабардың) ұзындығы N блогын шифртекст блогына, сондай-ақ, кейбір ұзындығы N құпия кілтті пайдалана отырып түрлендіреді. Шифрлау процесі бірнеше қайталанатын раундтардан тұрады, әдетте, раунды K_i ішкі кілтке байланысты, арнайы ереже бойынша бастапқы K кілттен өндіріліп алынатын, бірдей раундтық функциямен анықталады.

Блоктық шифрлардың ең көп таралған түрлері, *SP-желісі* және *Фейстель желісі,* схемалық сұлбасы [А.1.1.1-сурет] келтірілген. Бұл сұлбалардың екеуі де Клод Шеннон өз жұмысында анықтаған шифрлеу түрлендірулерін құрудың екі принципін - *шашырату және араластыруды* сипаттайды. Араластыру ашық және шифрленген мәтіндердің статистикалық және аналитикалық қасиеттерінің өзара байланысын қалпына келтіруді қиындатады, ал шашырату ашық мәтіннің бір белгісі шифрмәтіннің үлкен белгілерінің санына әсерін тудырады, бұл ашық мәтіннің статистикалық қасиеттерінің шифрмәтіннің қасиеттеріне әсерін реттеуге мүмкіндік береді. SP-желі мысалында P-блок шашырауды қамтамасыз етеді, ал шағын S-блоктардың жиыны араластыруға әсерін тигізеді. P-блок ретінде әдетте сызықтық функция таңдалады, ал S-блоктар шифрдың сызықты емес түрлендірулерін құрайды.

Шын мәнінде, S-блок – бұл векторлық (n, m)-функция, және де n, m-нің мәні үлкен емес, мысалы 4, 6, 8 бит. Мұндай шағын өлшемге қарамастан, "жақсы" криптографиялық қасиеттері бар S-блокты табу өте қиын. Көрнекі болу үшін F_2^8-ден барлық мүмкін 2^{2048} сәйкестендірулер бар, бұл қазіргі уақытта толық іріктеп таңдауға берілмейді!

1.2 SP-желісі

SP-желісі (ағылшынша substitution-permutation network, SPN) - итеративті блоктық шифрлардың маңызды түрлерінің бірі. SP-желі негізіндегі шифр кіріске блок пен кілтті алады және бірнеше ауысатын ауыстыру кезеңі (ағылш. substitution stage) мен алмастыру кезеңінен (ағылш. permutation stage) тұратын бірнеше раундты орындайды. Қауіпсіздікке қол жеткізу үшін бір ғана S-блок жеткілікті, бірақ мұндай блок жадтың үлкен көлемін талап етеді. Сондықтан P-блоктармен аралас шағын S-блоктар

қолданылады. Сызықсыз алмастыру кезеңі ашық мәтіннің биттері мен кілттің биттерін араластырып, Шеннон конфузиясын жасайды. Ауыстырудың сызықтық сатысы диффузияны туындататады.

S-блок (ағылш. substitution box немесе S-box) кіріс биттерінің шағын блогын басқа шығыс биттерінің блогына ауыстырады. Бұл ауыстыру кері қайтаруға кепілдік беру үшін өзара бір жақты болуы тиіс. S-блоктың мақсаты сызықты емес түрлендіруден тұрады, бұл сызықтық криптоанализді жүргізуге кедергі жасайды. S-блоктың қасиеттерінің бірі-лавиндік әсер, яғни кірісте бір биттің өзгеруі шығысында барлық биттердің өзгеруіне әкеледі.

P-блок (ағылш. permutation box немесе P-box) s-блоктың шығысындағы нәтижені кірісіне алады, барлық биттерді орындарымен ауыстырады және нәтижені келесі раундтағы S-блоктың кірісіне береді. P-блоктың маңызды қызметі бір S-блоктың шығысын мүмкіндігінше үлкен S-блоктардың кіріс арасында бөлу мүмкіндігі болып табылады.

Әрбір раунда бастапқы кілттен алынған өз кілтін пайдаланылады. Мұндай кілт раундтық деп аталады. Ол бастапқы кілтті тең бөліктерге бөлу арқылы және барлық кілтті қандай да бір түрлендіруімен алынуы мүмкін.

1.3 Фейстель желісі

Фейстель желісі – бұл *F* еркін функциясын көптеген блоктарға ауыстырудың жалпы әдісі. Ол циклды қайталанатын раундты ұяшықтардан тұрады. Әрбір раундтың ішінде ашық мәтіннің блогы екі тең бөлікке бөлінеді.

Раундтық функция мәтін блогының бір жартысын, яғни оң бөлігін алып (суреттің оң жағы), оны K_i кілтін пайдаланып түрлендіреді және екінші жарты нәтижені болдырмайтын НЕМЕСЕ (XOR) операция арқылы біріктіреді. Бұл кілт *K* бастапқы кілттен өндіріліп алынады және әр раундта әр түрлі болады. Содан кейін жарты блоктар орындармен ауысады (әйтпесе блоктың тек бір жартысы ғана өзгереді) және келесі раундқа беріледі. Фейстель желісін түрлендіру кері операция болып табылады.

F функциясы үшін белгілі бір талаптар бар:

• оның жұмысы лавинды эффектіге әкелуі керек;

• XOR операциясына қатысты сызықсыз болуы керек;

Бірінші талап орындалмаған жағдайда, желі дифференциалды шабуылдарға ұшырайды (ұқсас хабарламалардың ұқсас шифрлары болады). Екінші жағдайда шифр сызықты және шифрді ашу үшін сызықтық теңдеулер жүйесінің шешімі жеткілікті.

Мұндай құрылым айтарлықтай артықшылыққа ие: шифрлеу/шифрін кері ашу процедуралары сәйкес келеді, тек бастапқы кілттің туындылары кері тәртіпте пайдаланылады. Бұл дегеніміз, бір блок шифрлау үшін де, шифрді кері ашу үшін де қолданылуы мүмкін, яғни шифрді іске асыру әлде қайда жеңіл болады. Схеманың кемшілігі – әрбір раундтағы блоктың жартысы ғана өңделеді, бұл раундтардың санын көбейту қажеттігіне әкеледі.

1.4 Потоктық шифрлар

Кеңінен қолданылатын потоктық шифрдің моделі – гаммалау шифірін келтірейік. Мұндай жүйелердің негізінде ашық мәтінге (шифрленетін хабарлама) кілттік (гамма) тезбекті "біріктіру" әдісі жатыр (мысалы, екілік модуль бойынша қосу). Клод Шеннон жұмыстарынан, егер кілттің ұзындығы хабарлама ұзындығына тең болса және кілт кездейсоқ және теңықтималды таңдалып, бұл ретте бір рет ғана қолданылса, онда бұл шифрлау жүйесі шифртекст негізінде шабуылдарға абсолютті төзімді болып табылады. Мұндай модель кең түрде қолданылмайды, себебі хабарлама ұзындығына тең кілтті генерациялап алу және оны жіберу өте қиын, сондай-ақ әзірлеушілер алдында қысқа кездейсоқ кілттер тізбегінен кейбір ұзын тізбекті (гамма) алу міндеті тұр, және де ол кездейсоқтыққа жақын болу керек. Осы тізбектің қасиеттеріне шифрлардың криптографиялық тұрақтылығы байланысты екенін байқаймыз. Потоктық шифр компоненті ретінде әдетте кері байланысы бар жылжыту регистрлері қолданылады. Олардың жұмысының жалпы сұлбасы [А.1.4.1-сурет] келтірілген, мұнда: n айнымалысының f-булевтік функциясы кері байланыс функциясы болып табылады.

Жұмысты бастамас бұрын, n биттермен регистрдің бастапқы жағдайын толтырады. Бұдан әрі әрбір жұмыс тактісінде келесі мән есептеледі: $\alpha = f(x_{n-1}, \ldots, x_0)$, содан кейін регистрдің барлық биттері солға жылжиды, бұл ретте соңғы оң жақтағы битке α мәні жазылады, ал шеткі сол бит кезекті шығыс тізбегінің $u = \{u_0, u_1, u_2 \ldots\}$ битіне айналады.

Сызықтық кері байланысы бар регистрлер (LFSR) кеңінен таралуда, яғни, f сызықты, сондай-ақ, $f(x_{n-1}, \ldots, x_0) = \langle c, x \rangle$, мұнда $c \in F_{2^n}$. Кері байланысы бар кез-келген регистрден туындайтын тізбек әрқашан периодты. Шын мәнінде кез келген периодты тізбекті сәйкес ұзындықты LFSR тудыруы мүмкін екенін көру оңай. Бұл жағдайда тізбектің $\mathcal{L}_u$ сызықты күрделілігі - оны генерациялайтын LFSR-дің ең аз ұзындығы. Тізбектің сызықтық күрделілігі — оның аналитикалық құрылысының күрделілігін сипаттайтын негізгі параметр.

Естеріңізге сала кетейік, "жақсы" гамма жасау үшін тек бір LFSR ғана пайдаланылмайды. Шынында да, егер біз кері байланыс функциясы $f(x) = \langle c, x \rangle$, $c \in F_{2^n}$, білсек, онда сызықтық теңдеулер жүйесін шешу арқылы регистрдің бастапқы күйін қалпына келтіру үшін, тізбекті биттер жиыны жеткілікті. Бастапқы жағдайдағы биттер, әдетте, шифрлардың құпия кілті болып табылады.

Сонымен қатар, кез келген периодтты тізбек үшін сызықтық кері байланыс функциясын табуға мүмкіндік беретін күшті нәтиже белгілі. Мысалы, біз кездейсоқ периодтты тізбектің ұзын бөлігін қолға түсірдік. Ол кезде Берлекэмпа — Мессидің кең танымал алгоритмі көмегімен соңғы тізбектің ұзындығынан полиномиальды уақыт ішінде рекурсия заңын табуға болады, ол тізбектің осы бөлігін шығаратын сызықтық регистрді табуға эквивалентті. Бұл ретте, егер тізбектің ұзындығы $2\mathcal{L}$ - дан кем емес болса, мұндағы $\mathcal{L}$ оның сызықты күрделілігі, онда тізбек бөлігі бізге белгілі табылған LFSR барлық шексіз тізбекті өндейді.

Екінші жағынан, өңделетін тізбектің сызықтық күрделілігі регистрдің кез келген бастапқы жағдайында — белгісіз кілтте жоғары болуы тиіс. Осыған байланысты кейбір күрделенулерді пайдаланады. Сызықтық кері байланысы бар жылжу регистрлері негізінде құрылған генераторлардың екі негізгі моделін көрсетуге болады [А.1.4.2-сурет].

2 Актуалдылық

Блоктық және потоктық шифрлар конфиденциалды сандық ақпаратты қорғауда кеңінен қолданылады. Блоктық және потоктық шифрларға қолданылатын көптеген шабуылдар бар екені бізге белгілі. Ең қарқынды жүргізілетін шабуылдардың бірі алгебралық шабуылдар. Яғни, шифрды қарапайым алгебралық жүйеге қою арқылы, белгілі алгебралық тәсілдерді қолданумен шифрды шешіп алуға мүмкіндік туып отыр. Және де шифрмәтін мен ашықмәтін арасындағы статистикалық байланыстарды негізге ала отырып, шифрдың өзектілігін жоюға қадамдар жасалуда.

Асимметриялық және симметриялық примитивтерді қолдану барысында, симметриялы шифрлау жүйесі асимметриялы шифрлаудан жоғарғы жылдамдығының арқасында, кілтті берудің әлсіз механизміне қарамастан акуталды болып табылады.

Мемлекеттік дәрежедегі құпияларды сақтауда қолданылатын стандарттар алгоритмі, негізінен симметриялық блоктық шифрлауды қолданады. Осы шифрларда пайдаланатын S-блоктар, шифрлау алгоритмінің негізгі этаптарының бірі. Өйткені, шифрдің криптоталдауға тұрақтылығы ең негізгі екі шабуылға, яғни дифференциялдық және сызықтық шабуылдарға төтеп беруінде. Осы шабуылдарға криптотұрақтылық, осы күннің өзекті тақырыптарының біріне айналып отырған, сызықсыз ауыстыру түйіндерінің жоғарғы криптографиялық қасиеттері негізінде қол жеткізіледі. Ауыстыру түйіндерінің осы жұмыста сипатталатын қасиеттерінің арқасында блоктық шифрларды қолдану актуалдылығы әлі де жоғарғы деңгейде.

Жоғарыда айтылған шабуылдардың, жақсы қасиеті бар ауыстыру түйіндерін қолданатын блоктық шифрларға жасалынып, оны сындыру тек теориялық тұрғыда қол жеткізіліп, практикалық іске асырылуы әлі де мүмкін емес деңгейде. Яғни, осындай шабуылдарға тұрақтылығының арқасында ауыстыру блоктары өзектілігін жоғалтпаған және де булевтік функцияның шексіз қасиеттерінің арқасында зерттеу жұмыстарын ары қарай жүргізіліп, оны абсолют тұрақты деңгейге жеткізілуі негізгі жұмыстардың бірі.

3 Векторлық булевтік функцияның криптографиялық қасиеттері, криптографиялық алгоритмдердің сенімділігіне әсері

Жарты ғасыр бойы шифрлеу жүйелерінде қолданылатын булевтік функцияларына көптеген талаптар қалыптасты. Осы талаптарды қанағаттандыратын функциялар "криптографиялық булевтік функциялары" деп атала бастады. Бұл тарау булевтік функциясының негізгі криптографиялық қасиеттерін сипаттауға арналған: *жоғары алгебралық дәреже, теңестірілу және толықтай теңестірілу, лавиндік сипаттамалар, сызықтық құрылымдардың жоқтығы, корреляциялық иммундық және тұрақтылық, жоғары сызықсыздық, алгебралық иммуннитет.* Шифрлардың компоненттері болып табылатын булевтік функциясының белгілі бір осалдықтарын пайдаланатын блоктық және ағынды шифрларға шабуылдар негізінде қасиеттердің деректерін қалыптастыру мәселелері зерттеледі; осы шабуылдардың негізгі идеялары келтіріледі. Әрбір қасиетке негізгі теориялық нәтижелер қысқаша қарастырылып, осы салада ашық мәселелер тұжырымдалды. 3.1.1-кесте осы тараудың негізгі мазмұнын көрсетеді.

№	Қасиеті	Мақсаты
1.	Жоғары алгебралық дәреже	Генерацияланатын тізбектің сызықтық күрделілігін арттыру; шифрды сипаттайтын сызықты емес теңдеулер жүйесінің дәрежесін арттыру
2.	Теңестірілу	Потоктық генераторлар шығаратын тізбектердің статистикалық қасиеттерін жақсарту
3.	Толықтай теңестірілу	
4.	Лавинды сипаттамалары	Кіріс айнымалы мәндерінің аз санының мәндерін өзгерткен кезде, шығыс мәндердің үлкен санының мәндерін өзгертуді қамтамасыз ету
5.	Корреляциялық иммундық, тұрақтылық	Потоктық шифрлерге корреляциялық шабуылдарды жүргізуге кедергі тудырады, ал блоктық шифрлау алгоритмінің шығу тізбегінің статистикалық сапасына әсер етеді.
6.	Жоғарғы сызықсыз дық	Потоктық шифрлерге жылдам корреляциялық шабуылды жүргізуге, ал блоктық шифрлерде сызықтық криптоталдауға кедергі тудырады

7.	Алгебралық иммуннитет	Шифрларға алгебралық криптоанализді жүргізуіге кедергі келтіреді

3.1.1-кесте: Қарастырылатын криптографиялық қасиеттер және олардың тағайындалуы.

3.1 Жоғары алгебралық дәреже

Комбинациялаушы және фильтрлаушы h функциясы ретінде қайсысының дәрежесі аз емес, соны таңдау керек. Алдымен $L_1, \ldots, L_n$ ұзындықтан тұратын кері сызықтық байланысы бар n регистрден тұратын комбинациялаушы генераторды қарастырайық. Комбинациялаушы h функциясы алгебралық нормалды формада берілсін: $h(x_1,\ldots,x_n) = \oplus_{k=1}^{n} \oplus_{i1,\ldots,ik} a_{i1,\ldots,ik} x_{i1}\ldots x_{ik}$, мұндағы $\{i_1,\ldots,i_k\} \subseteq \{1, \ldots, n\}$ және $a_{i1},\ldots,i_k \in F_2$. Содан кейін өңделетін тізбектің сызықтық күрделілігі $\mathcal{L}$ регистрлердің ұзындығы арқылы жоғарыдан бағаланады:

$$\mathcal{L} \leq \sum_{k=1}^{n} \sum_{i_1,\ldots,i_k} L_{i1} \ldots L_{ik} ,$$

бұл ретте, осы бағалауға қол жеткізу шарттары белгілі: егер L_i генерацияланатын $LFSR_i$ тізбектің сызықтық күрделілігімен сәйкес келсе, кез-келген i және $L_1,\ldots,L_n$ саны өзара жай. АНФ дәрежесі жоғары болған сайын, соғұрлым үлкен сызықтық күрделілікті алуға болады.

Фильтрлеуіш модель жағдайында ұқсас дәл нәтиже жоқ, дегенмен де фильтрлаушы функцияның $\deg(h)$ дәрежесі арқылы генерацияланатын тізбектің сызықтық күрделілігінің нәтижесі белгілі. Дәлірек айтқанда $\mathcal{L} \leq \sum_{i=0}^{\deg(h)} C_L^i$, мұндағы $\mathcal{L}$ — регистр ұзындығы, ал C_L^i — биномиалды коэффициент. Бұдан бөлек егер $\mathcal{L}$ – жай сан болса, онда төменнен бағалаған дұрыс: $\mathcal{L} \geq C_L^{\deg(h)}$.

Блоктық шифрларда, үлкен дәрежелі функцияларды таңдау керек. «$\deg(F)$ параметрі үлкен болуы тиіс. Блоктық шифрларда бұл шарт, әдетте, шифр құрылымын талдау жолымен құрылған кілттің биттеріне арналған теңдеулер жүйесі үшін, соның ішінде оның компоненті ретінде қолданылатын F функциясы жоғарғы алгебралық дәрежеге ие болуы үшін қойылады. Жүйенің дәрежесі жоғары болған сайын, оны шешу қиын, яғни кілтті анықтау күрделі».

3.2 Теңестірілу

Анықтама. Булевтік функция f, n айнымалысынан теңестірілген деп аталады, егер оның салмағы 2^{n-1} тең болса, сондай-ақ функция 0 және 1 мәндерін бірдей қабылдайды.

Бұл, потоктық шифрларда булевтік функциялар қолданылатын ең табиғи қажетті қасиеттердің бірі. Егер булев функциясы теңестірілген болса, онда ол 0 немесе 1 мәнін алатын ықтималдық бірдей және 1/2 тең. Бұл функция кірісі мен шығысы арасындағы статистикалық тәуелділікті әлсіретуге мүмкіндік береді. Әйтпесе, криптоаналитикада ықтималдық арақатынасын пайдалана отырып, шифрлардың криптоанализін жүргізу мүмкіндігі бар.

Бұл анықтама векторлық жағдайға жалпыланады.

Анықтама. Векторлық (n, m)-функция F теңестірілген деп аталады, егер $|F^{-1}(y)| = |\{x \in F_2^n : F(x) = y\}| = 2^{n-m}$ кез-келген $y \in F_2^m$.

Бұл ретте келесі тұжырымдаманы келтірсек болады:

Векторлық (n, m)-функция F ии $v \in F_2^m$, $v \neq 0$ компоненті функциялары теңестірілген болса.

Сондықтан, $n = m$ теңестірілген функциялардың сыныбы бір-бірімен бірдей функциялардың сыныбымен сәйкес келеді. Әдетте, олар блоктық шифрларда S-блоктар ретінде бір ретті шифрлеуді қамтамасыз ету үшін ең үлкен қызығушылық тудырады.

3.3 Толықтай теңестірілу

Толықтай теңестірілген булевтік функцияның қасиеті, қарапайым теңестірілудің табиғи жалпы түрі болып табылады, сол кезде осы функция фильтрлаушы генератор есебінде жұмыс жасайды.

n айнымалысынан f — фильтрлаушы функция генераторы болсын. $\ell + n - 1$ ұзындықтағы $x = (x_1,..., x_{\ell+n-1})$ — кіріс тізбектік бөлігі, мұндағы ℓ – кездейсоқ натурал сан. Содан кейін, генератор ℓ ұзындықты, $u = (u_1,..., u_\ell)$ тізбек бөлігін өндіреді, мұндағы $u_i = f(x_i , x_{i+1},..., x_{i+n-1})$, $i = 1, ... , \ell$. f функциясына және ℓ санына векторлық f_ℓ, $(\ell + n - 1, \ell)$ – функциясын анықтаймыз және жоғарыда айтылған ереже бойынша x векторына u векторын сәйкестендіреміз.

Анықтама. Булевтік функция f толықтай теңестірілген деп аталады, егер кез-келген ℓ натурал санына f_ℓ функциясы теңестірілген болса.

Атап айтқанда, егер функция толықтай теңдестірілген болса, онда ол қарапайым теңдестірілген болып табылады. Кері жағдайда дұрыс емес.

f булевтік функцияның тыйым салынуы деп, кез-келген ℓ үшін, $u = (u_1, ... , u_\ell)$ векторы аталады және де $f_l^{-1}(u)$ кескіндері бос болса. Келесі теорема функцияға тыйым салу терминдерінде толықтай теңестірілу критерийлерін көрсетеді.

Теорема. Булевтік функциясы толықтай теңдестірілген, егер ол тыйым салынбаған функция болса.

Генератордың фильтрлаушы функциясында тыйым салудың болуы оны жақсы статистикалық қасиеттері бар тізбектердің пайда болуы тұрғысынан "әлсіз" ететіні интуитивті түсінікті. Алайда, толықтай теңестірілген фильтрлаушы функция, кіріс тізбегінің қасиетін генерацияланатын тізбектің қасиетіне ауыстыруы мүмкін. Мысалы, фильтрлаушы функция тыйымдарды толықтай теңдестірілген кезде ғана сақтайды. "Тиісінше, егер кіріс функциясына кездейсоқ тізбектен "алыс" тізбек түссе, онда оның статистикалық қасиеттері нашар болады.

Егер фильтрлаушы функция өзінің бірінші және/немесе соңғы айнымалысы бойынша сызықты болса, онда ол толықтай теңдестірілген. Бірақ кері жағдайда бұл дұрыс емес, өйткені олардың шеткі айнымалыларына сызықсыз тәуелді толықтай теңдестірілген функциялардың конструкциялары табылды. Мұндай функциялардың кең кластарын іздеу өзектілігі сүзгілеуші ретінде бірінші немесе соңғы айнымалы функциялар бойынша сызықты пайдаланатын фильтрлеуші генераторларға инверсиялық шабуыл деп аталатындығымен расталады.

3.4 Лавиндық сипаттамалары

Булевтік функциясының лавиналық сипаттамаларының концепциясы шифрлеу түрлендірулерін құру, яғни Шеннон принциптерінің бірін, атап айтқанда шашырату принципін бейнелейді. *Анықтама.* Булевтік функция f, n айнымалысынан қатаң лавинды критериді қанағаттандырады, егер кез-келген бағыттағы $a \in F_2^n$, мұндағы wt(a) = 1, туындысы $D_a(f)$ теңестірілген болса.

Егер барлық (n, m)-векторлық функциялардың координаталық функциялары SAC-ты қанағаттандыратын болса, онда бір кіріс биті 1/2 ықтималдығымен өзгергенде әрбір шығыс биттері өзгереді. Демек, шығыс биттерінің жартысы өзгереді деп күтуге болады.

Анықтама. Булевтік функция f, n айнымалысынан k дәрежені тарату критериін қанағаттандырады, егер кез-келген бағыттағы $a \in F_2^n$, мұндағы $1 \leq$ wt(a) $\leq k$, туындысы $D_a(f)$ теңестірілген болса.

Анықтама бойынша PC(1), SAC-пен сәйкес келеді. Алдын ала айта кетсек, PC(n)-ді қанағаттандыратын функция – бұл бент-функцияның дәлділігінде. Егер функция осы өлшемдерді қанағаттандырса, онда бұл кіріс векторының бірнеше биттердегі өзгеруі функцияның мәнін 1/2 ықтималдығымен өзгертетінін білдіреді.

Қатаң лавинді критерий және оны жалпылау «зерттелетін криптографиялық функциялар үшін жергілікті қасиеттер индикаторлары болып табылды». Дұрыс талап етсек орта есеппен функциялардың «жақсы» лавиннды сипаттамалары болды, егер автокорреляцияның модуль функциялары $\Delta_f(a)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus f(x\oplus a)}$-ға тең немесе векторлардың көпшілігі үшін $a\in F_2^n$ нөлге жақын.

Анықтама. Булевтік функция f, n айнымалысынан глобалды лавинды сиппаттамасы (GAC) деп $\sigma_f = \sum_{a\in F_2^n}\Delta_f^2(a)$ и $\Delta_f = max_{a\in F_2^n, a\neq 0}\ \Delta_f(a)$ саны аталады.

Бұл шамалар неғұрлым аз болса, шифрде пайдалану функциясы соғұрлым жақсы, себебі GAC лавинды көрсеткіштерін орташа көрсетеді.

3.5 Корреляционндық иммунндық және тұрақтылық

Осы тармақта қарастырылған қасиеттер әртүрлі қолданбалы есептерден пайда болды, бірақ басқа қасиеттермен тығыз байланысты болып шықты. Корреляциялық иммундық терминін T. Siegenthaler енгізді. Ол генератордың потоктық шифрдегі құрамдастырылған функциясы ретінде қолданылатын корреляциялық иммундылықтың жоғары тәртібі бар функциялар шифрды корреляциялық шабуылға төзімді етеді. Шабуылдың мәні функцияның мәнін біле отырып, функция туралы ақпарат алуға болатын ауыспалы құрамдастырылған функцияның ішкі жиынтығын іздеуден тұрады. Тұрақты функциялар 80-ші жылдары ашық әдебиетке енгізілді, «қателерге қатысты тұрақты таратылған есептеулер және кванттық-криптографиялық байланыс арналары үшін ортақ кілттерді жасау сияқты зерттеу салаларымен байланысты болды». Потоктық шифрларда генератордың комбинациялаушы функциясы ретінде тұрақтылық қасиеті бар функцияны қолданған дұрыс. Бұл ретте, тұрақтылық тәртібі жоғары болған сайын, шифрдың корреляциялық криптоталдауға тұрақтылығы артады. Комбинаторика тілінде берілген қасиеттердің формальды анықтамаларын келтірсек. Алдымен ішкі функция түсінігін анықтайық. f булевтік функциясының $x_1, \ldots, x_n$ айнымалысынан ішкі функциясы деп f-тан алынған ауыстырудың $x_{i_1},\ldots,x_{i_k}$ айнымалысының орнына тұрақты $a_1, \ldots, a_k$ константаларды қабылдайтын 0 немесе 1 мәндері. Бұндай ішкі функция $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$-пен беріледі.

Анықтама. Булевтік функция f, k ретті корреляциялық-иммунды деп аталады, егер $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ ішкі функцияның салмағы, кез-келген $1 \leq i_1 < \ldots < i_k \leq$

n индекстердің жиынтығында, кез-келген $a_1, \ldots, a_k \in$ F2 мәнінде wt($f^{a_{1,\ldots,a_k}}_{i_{1,\ldots,i_k}}$) = wt($f$)/$2^k$ арақатынасын қанағаттандырса.

Басқаша айтқанда, Булевтік функция f, k ретті корреляциялық-иммунды деп аталады, егер P[f = 1] = P[$f^{a_{1,\ldots,a_k}}_{i_{1,\ldots,i_k}}$=1], мұндағы P – ықтималдылық функциясы, кейбір кіріс биттерінің мәні, функцияның мәні жайлы статистикалық ақпаратты бермейді.

Анықтама. Булевтік функция f тұрақты деп аталады (k-эластикалық), егер оның кез-келген ішкі функциясы k айнымалыдан көп емес жылжумен алынса теңдестірілген болып табылады.

Булевтік функция f, k ретті теңдестірілген және корреляционды-иммунды кезде ғана тұрақты екеніне көз жеткізу қиын емес.

Корреляциялық шабуыл идеясы

f — комбинациялаушы функция генераторы болсын, $L_1, \ldots, L_n$ ұзындықтағы, $LFSR_1$, . . ., $LFSR_n$ - кері байланысы бар сызықтық жылжымалы регистр, сәйкесінше u=u_0, u_1, u_2 – регистрдің шығыс тізбегі. Криптоталдаудың күрделілігі регистірдің бастапқы жағдайын іріктеу, $2^{L_1+\cdots+L_n}$ ретінде бағаланады. Егер регистр дұрыс құрылса, онда u тізбегі кездейсоқтыққа жақын болып табылады, сондықтан P[u_i = 0] ≈ 1/2 деп санауға болады. Сәйкесінше, егер z = z_0,z_1,z_2,... өздігінен u тізбекке тәуелді емес болса, онда P [u_i = z_i] ≈1/2 деп санауға болады, өйткені P[u_i = z_i] = P[u_i = 0] P[z_i = 0]+ P[u_i = 1] P[z_i = 1] ≈ 1/2 (P[z_i = 0] + P[z_i = 1]) = 1/2.

Мысалы, f функциясы $\ell(x_1, \ldots, x_n) = x_1$ функциясымен корреляцияланады және P[f = ℓ] = 1/2 + $\varepsilon \neq$ 1/2 екенін білдіреді. Сонда $LFSR_1$ регистрдің белгісіз бастапқы күйін қалпына келтіруге болады. Бұл үшін бірінші регистрдің бастапқы белгісіз жағдайын қалпына келтіріп және осы z = z_0, z_1, z_2, . . . регистрдің шығыс тізбегін генерациялап, z_i = u_i қанша рет орындалғанын есептеуге болады. Егер регистрдің бастапқы жағдайы дұрыс емес берілген болса, онда P[z_i = u_i] ≈ 1/2, ал дұрыс болса P[z_i = u_i] ≈ 1/2 + ε. Осылайша, корреляция |ε| мәні неғұрлым көп болса, соғұрлым біз регистрдің дұрыс күйін табамыз. Сондай-ақ, іздеу күрделілігін $2^{L_1}+ 2^{L_1+\cdots+L_n}$ деңгейіне дейін төмендеттік. Егер f пен басқа айнымалылардың арасындағы корреляция болса, күрделілік тағы да төмендеуі мүмкін. Егер f функциясының $\ell(x) = x_i$ функциясымен ешқандай корреляциясы болмаса, онда басқа сызықтық функциялармен корреляцияны іздеуге болады және де wt(c) = k шағын, айталық c = (1, . . . , 1, 0, . . . , 0). Сонда іздеудің күрделілігі $2^{L_1+\cdots+L_k} + 2^{L_{k+1}+\cdots+L_n}$ дейін төмендейді. Бірақ егер k жеткілікті үлкен болса, онда криптоаналитик үшін көп пайда болмауы да мүмкін.

f функциясы бар фильтрлаушы генераторды сол f функциясымен арнайы құрылған комбинациялаушы генераторға алып келуге болады. Бұл жаңа генератор белгілі бір регистрдің бастапқы күйін толтыру арқылы сол тізбекті өндіріп шығарады. Демек, корреляциялық шабуылды фильтрлаушы генераторлар жағдайына жалпылауға болады.

Негізгі теоремалар және сызықтық емес байланыс

Тұжырымдама. k ретті корреляциялық-иммунды булевтік функциясы үшін k ретті барлық $\ell < k$-ға корреляциялық-иммунды болып табылады.

Осы мәлімдемеге сүйене отырып cor (f) функциясының корреляциялық иммундық тәртібін анықтайды.

cor(f) = max{$0 \leq k \leq n : f$ - корреляциялық иммундық тәртіп.

Келесі танымал теорема корреляциялық-иммундық және тұрақты функциялардың спектральдық сипаттауын береді.

Теорема (спектральды сипаттама). n айнымалылардың f булевтік функциясы болсын. cor (f) = k егер барлық векторлар үшін $W_f(y) = 0$ болса ғана жарамды, және $1 \leq \text{wt}(y) \leq k$. Сонымен қатар, егер $Wf(0) = 0$ болса, f теңестірілген болып табылады.

Бұл теорема корреляция-иммундықтың k ретті функцияларын анықтайды және потоктық генератордың комбинациялаушы функциясы ретінде қолданғанда корреляциялық шабуылға қарсы тұра алады. Шынында да, шабуыл жасау үшін $\ell(x) = \langle c,x\rangle$ сызықтық функциясын табу керек, сондай-ақ комбинация функциясының P [$f = \ell$]≠ 1/2 корреляциясы бар. Өйткені P[$f = \ell$] = (2^n − d(f,ℓ)) /2^n = 1/2 + (2^{n-1} − d(f, ℓ)) /2^n ≠ 1/2 функциясы d(f, ℓ) ≠2^{n-1}-ге эквивалентті. Сонымен қатар, f және сызықтық функция $\ell(x)$ = $\langle c, x\rangle$ арасындағы қашықтықты d(f, ℓ) = $2^{n-1} - Wf(c)/2$ ретінде көрсету оңай. Осылайша, егер d(f,ℓ) ≠ 2^{n-1} және $Wf(c) \neq 0$ болса, біріктіру функциясының тұрақтылық реті жеткілікті жоғары болады. Онда осы шифр бойынша корреляциялық шабуыл жасау қиынға соғады.

Cor(f) және deg(f) функциясының дәрежесі арасындағы байланыс келесі теоремада көрсетілген.

Теорема (Siegenthaler). n айнымалылардың f булевтік функциясы болсын.

1. Егер cor(f) = k болса, онда deg(f) + $k \leq n$ орындалады.

2. Егер cor(f) = k, f теңдестірілсе және $k \leq n$ - 2 болса, онда deg(f)+$k \leq n - 1$ орындалады.

Теоремадан функцияның дәрежесі неғұрлым жоғары болса, оның корреляциялық иммундық реті аз және керісінше төмен болса көп. Бірақ, біз

көргеніміздей, бұл параметрлердің екеуі криптографиялық генераторлардың күрделілік функциялары үшін жоғары болуы тиіс.

Салдары. n айнымалылардың f булевтік функциясы болсын. Егер cor(f) = n болса, онда $f \equiv$ const. Егер cor(f) = n - 1, онда $f(x) = x_1 \oplus \ldots \oplus x_n \oplus$ const.

Теорема (Фон-Дер-Флааcс). n айнымалылардың f теңестірілмеген булевтік функциясы болсын. Сонда cor(f) $\leq (2n/3) - 1$.

Мұнда N_f корреляциялық-иммундық функциялардың сызықтық емес екендігін атап өту керек.

Теорема (cor(f) және N_f байланысы). n айнымалылардың f булевтік функциясы болсын.

1. Егер cor(f) = k, $k \leq n$ - 1 болса, онда $N_f \leq 2^{n-1} - 2^k$ орындалады.

2. Егер cor(f) = k, f теңдестірілсе және $k \leq n - 2$ болса, онда $N_f \leq 2^{n-1} - 2^{k+1}$ орындалады.

Теоремадан көріп отырғанымыздай, функцияның сызықтығы тұрақтылық реті өсу тәртібімен азаяды. Бұл cor(f) ұлғайған сайын, функцияның нөлдік Уолш-Адамар коэффициенттері үлкейе бастайды, бұл Парсевалдың теңдігіне байланысты максималды $|Wf\ (a)|$ мәнінің үлкеюіне, сәйкесінше, сызықты емес төмендеуге алып келеді. Оның үстіне, cor(f) және N_f байланысы туралы теоремалардан бағалаудың қол жетімділігі қызықты және орынды. Егер анықталған функцияларды бағалауға қол жеткізілсе, онда $(n - 3)/2 \leq k \leq n - 2$, бірақ мұндай барлық мүмкін параметрлер үшін әлі ешқандай мысал табылмады.

3.6 Жоғары сызықсыздық

Анықтама. n айнымалылардың f булевтік функциясының сызықтығы - n айнымалысынан барлық аффинді функцияларының f-ке дейінгі Хэмминг қашықтығына тең N_f шамасы.

Біз ерікті функция d(f,$\langle c, x\rangle$) = $2^{n-1} - W_f\ (c)/2$ мен сызықтық функциясы арасындағы қашықтықты байланыстырдық. Осыған сүйенсек, сызықты емес f, Уолша — Адамар коэффициенттері бойынша көрінеді: N_f = d(f, $\mathcal{A}n$) = $2^{n-1} - max_{c \in F_2^n} |W_f\ (c)|/2$. Сонымен қатар, Парсеваль теңдігі бойынша бағалауды төменнен көрсетуге болады: $max_{c \in F_2^n} |\ |Wf\ (c)| \geq 2^{n/2}$. Осылайша, функцияның сызықтығы әрқашан $Nf \leq 2n$ - 1 - $2n$ / 2-1 теңсіздігін қанағаттандырады.

Анықтама. *Максималды сызықсыз* функция деп, оның сызықсыз болуы мүмкін максималды мәнге жетуін айтады. Айнымалы функциялардың жұп саны кезінде олар *бент-функциялар* деп аталады.

Булевтік функцияның сызықсыздық мәні неғұрлым жоғары болса, онда оны потоктық және блоктық шифрларда пайдаланудың артықшылығы бар. Мұнда әртүрлі шифрлерге екі шабуыл жасалуын келтіреміз.

Жылдам корреляциялық шабуыл идеясы

Бұл шабуылдың түрі комбинациялаушы генераторға қарапайым корреляциялық шабуылдан кейін пайда болды.

Корреляциялық және жылдам корреляциялық шабуыл үшін $\ell(x) = \langle c, x \rangle$ сызықтық функцияны табу керек, оның f корреляциясы бар, яғни $P[f = \ell]=1/2 + \varepsilon \neq 1/2$. Ал шабуылдардың айырмашылығы, біз үшін $wt(c)$ мәнінің маңызы жоқ, тек қана $|\varepsilon|$ мүмкіндігінше көп болса болды.

Әрі қарай, $\varepsilon > 0$ (басқаша, ℓ орнына, $\ell \oplus 1$функциясын қарастырамыз) деп есептейміз. $u = u_0, u_1, u_2, \ldots$ генератормен өңделетін тізбек болсын. Сонда дұрыс тізбек дұрыс емес тізбекке кедергі келтіретін $1/2 - \varepsilon$ қателік ықтималдылығымен $z = z_0, z_1, z_2, \ldots$ нәтиже болсын, мұнда сол генератор арқылы алынатын, бірақ f-тың орнына комбинациялаушы функциясы ℓ болады. Біз ε-ні жеткілікті үлкен таңдағандықтан, қателік ықтималдығы аз болады.

Мысалы, біз $u_k, \ldots, u_{k+N-1}$ тізбегінің бөлігін бақылай аламыз. Барлық ықтимал $z_k, \ldots, z_{k+N-1}$ мәндер жиынтығы N ұзындығының сызықтық коды. Содан кейін, u тізбегінің фрагментін бақылап, қателерді түзету арқылы, z тізбегін қалпына келтіруге болады. Бұл z сызықты күрделіліктің u сызықтық күрделіліктен әлдеқайда төмен болатындығын және рекурсия заңы мен Берлекэмп - Месси алгоритмін қолданатын регистрдің бастапқы күйін қалпына келтіру үшін тізбек ұзындығының әлдеқайда қысқа бөлігін қолдану жеткілікті.

Афиндық функциялары бар f функцияның ε корреляциялық мәні оның сызықсыздығы арқылы төменнен бағалануы мүмкін екендігін бірден атап өтеміз: $|\varepsilon| \leq 2^n - 2N_f$. Демек, сызықсыздық неғұрлым жоғары болса, соғұрлым корреляцияның жоғары болуы, демек, модельденетін шу арнадағы қателіктің ықтималдығы соғұрлым үлкен, бұл комбинациялайтын f функциясы бар комбинациялаушы генераторға жылдам корреляциялық шабуыл жасауға мүмкіндікті азайтады.

Сызықты криптоталдау идеясы

1993 жылы жапондық криптограф М.Мацуи сызықтық криптоанализ деп аталатын DES шифрын талдау үшін статистикалық әдісті ұсынды. Біз қарапайым модификацияның идеясын сипаттасақ.

P, C, K – ашық мәтіннің, шифр мәтіннің блоктары және кейбір блоктық шифрдың кілті болсын. Шифрдың сызықтық жақындауы $1/2 + \varepsilon, \varepsilon \neq 0$

ықтималдықпен орындайтын, $\langle \alpha, P\rangle \oplus \langle \beta, C\rangle = \langle \gamma, K\rangle$ қатынасы, мұндағы α, β, γ - тиісті ұзындықтағы екілік векторлары. .

1-алгоритм. Сызықтық криптоталдау

Шифрдың сызықтық жақындауын $|\varepsilon|$ барынша көп болатындай табамыз.

2. Белгісіз тұрақты K кілт үшін N-нен (P, C) жұпты таңдаймыз.

3. Әрбір жұп үлгілері үшін 1-қадамда таңдалған коэффициенттің сол жақ бөлігінің мәнін есептейміз. N_0 – алынған нөлдер саны, ал N_1 – бірлер саны болсын, $N_0 + N_1 = N$.

4. $\langle \gamma, K\rangle = 0$, егер $(N_0 - N_1) > 0$ және $\langle \gamma, K\rangle = 1$ деп есептейік.

Нәтижесінде белгісіз кілттің биттеріне бір сызықты қатынасты табамыз, сәйкесінше толық іздеуді 2^k-дан 2^{k-1}-ге дейін төмендете аламыз, мұнда k - кілттің биттерінің саны. Сызықтық криптоталдандырудың бұдан басқа күшті модификациясы бар. Ол сізге дереу белгісіз негізгі кілт биттердің тобын табуға мүмкіндік береді, бірақ іздеу мәні бұрынғыша болып қалады. Бұнда сызықты жақындауға барлық шифр емес, тек оның бөліктері қолданылады.

Әдістің негізгі күрделілігі сызықты жақындауды табу болып табылады. Практика жүзінде іске асырылуы былай болады: S-блоктар үшін орындалатын қатынастарды талдайды, содан кейін оларды бірнеше раундтармен және көптеген P, C, K биттерге кеңейтеді.

Шифрдың S-блогы F функциясының (n, m) векторымен берілсін. $p = 1/2 + \varepsilon$, мұнда $\varepsilon \neq 0$ ықтималдығымен орындалатын $\langle a, x\rangle \oplus \langle b, F(x)\rangle = 0$ түріндегі қатынасты табу керек. $p = \mathrm{P}[\langle a, x\rangle = \langle b, F(x)\rangle] = 1/2 + (2^{n-1} - \mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle))/2^n$ деп жазайық. Барынша сәтті шабуыл жүзеге асыру мақсатында, барлық мүмкін нөлдік емес $a \in F_2^n$, $b \in F_2^m$ үшін, $|\varepsilon|$-нің мәнін ұлғайтып, $\mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle)$ арақашықтығын кішірейту керек. Тиісінше, осы шабуыл кедергісі ретінде барлық мүмкін нөлдік емес a, b мәні барынша үлкен болатындай, $\mathrm{d}(\langle a, x\rangle, \langle b, F(x)\rangle)$ минималды арақашықтықтағы, S-блоктар ретінде осындай векторлық функцияларды таңдау.

3.7 Алгебралық иммуннитет

n айнымалылардың f булевтік функциясы болсын. n айнымалылардың g булевтік функциясы деп, $fg = 0$ теңдігі орындалғандағы, f функциясының аннуляторын атайды .

Анықтама. f функциясының AI(f) алгебралық иммунитеті деп, $f \oplus 1$ функциясы немесе f функциясы үшін бірдей нөлге тең емес d дәрежелі g аннуляторы бар, d-ның ең аз саны болып табылады.

Алгебралық шабуыл идеясы

Булевтік функцияның алгебралық иммунитетінің анықтамасын түсіндірместен бұрын төмендегілерге көз жүгіртсек. Жалпы айтқанда, потоктық және блоктық шифрлер булевтік теңдеулер жүйесі ретінде сипатталуы мүмкін, онда ашық мәтін және шифр мәтінінің биттері қатысады. Осылайша, біз бір белгісіз кілтте бірнеше ашық мәтінді және шифрленген мәтінді білсек, оларды осы жүйеге ауыстыру арқылы оны шешуге болады. Мұндай жүйенің айрықша ерекшелігі - бұның бірлескен болуы, бірақ нақты шифрларда оны шешу қиынға соғады. Жалпы жағдайдағы сызықты емес булевтік теңдеулер жүйесін шешу мәселесі NP-қиын болып табылады.

Сызықты емес булевтік теңдеулер жүйесін шешудің бірнеше тәсілдері бар. Олардың бірін сипаттасақ. Сызықтық булевтық жүйелерді шешудің тиімді тәсілі ретінде Гаусс әдісі қолданылғандықтан, жалпы жағдайда сызықтық емес жүйені көп айнымалылар санында сызықтық жүйеге ауыстыру әрекеті болып табылады. Бұл әдіс линеаризация әдісі деп аталады. Алайда, жүйенің алгебралық дәрежесі неғұрлым жоғары болса, жалпы жағдайда соғұрлым көп айнымалы енгізуге тура келеді.

Тиісінше, бізде туындайтын мәселе мынада: біріншіден жүйенің шешімін жоғалтпай дәрежесін төмендетуге, содан кейін линеаризация әдісін қолдануға болады ма? 2003 жылы N. Curtois, W. Meier теңдеулер жүйесінің дәрежесін төмендетуге негізделген фильтрлаушы генераторының алгебралық криптоталдауын ұсынды. Кейінірек, бұл тәсіл комбинациялаушы генераторлар мен блоктық шифрларға жалпыланды, сондай-ақ булевтық функцияның алгебралық иммунитетінің соңғы ұғымы қалыптасты.

n айнымалыдан h функциясы бар фильтрлаушы генераторды қарастырамыз. Егер LFSR қолданатын рекурсия заңы $f(x) = \langle c,\ x\rangle$ болса, мұнда $c \in F_2^n$, онда векторлық сызықты $L^i(K)$, мұнда $L(x_{n-1}, \ldots, x_0) = (x_{n-2}, \ldots, x_0,\ f(x_{n-1}, \ldots, x_0))$, функциясының мәні фильтрлаушы функция кірісіне кезекті i-ші жұмыс тактісіне, $i = 1, 2, \ldots$, беріледі және $K = (k_{n-1}, \ldots, k_0)$ – регистрдің бастапқы күйі.

Егер $u_0, u_1, u_2, \ldots$ — генератордың шығыс тізбегі болса, онда

$$\begin{cases} u_0 = h\left(k_{n-1,\ldots,}k_0\right), \\ u_1 = h\left(L\left(k_{n-1,\ldots,}k_0\right)\right), \\ \ldots \\ u_0 = h\left(L^i(k_{n-1,\ldots,}k_0)\right), \\ \ldots \end{cases}$$

Егер тізбектің $\{u_i\}$ үзіндісі белгілі болса, осы теңдеулерден белгісіз K кілттің биттерінен алынған булевтік теңдеулердің сызықты емес жүйесі құрылады. Енді осы жүйенің теңдеулер дәрежесін төмендетуге кірісейік. Келесі шарттардың біреуі немесе екеуі де орындалды деп ойлайық:

1. $h(x)g(x) = t(x) \not\equiv 0$ және t дәрежесі кішкентай болатын g функциясы бар;

2. $h(x)g(x) \equiv 0$-ге тең шағын дәрежедегі $g \not\equiv 0$ функциясы бар.

Сонда жүйе теңдеулерінің дәрежесін келесідей төмендетуге болады:

• егер $u_i = 0$ болса, онда $h\ (L^i\ (k_{n-1}, \ldots, k_0)\ ) = 0$ орнына 1-шарт орындалатын, $t(L^i\ (k_{n-1}, \ldots, k_0)\ ) = 0$ теңдеуін қарастырамыз;

• егер $u_i = 1$ болса, онда $h\ (L^i(k_{n-1}, \ldots, k_0)) = 1$ орнына 2-шарт орындалатын, $g(L^i(k_{n-1}, \ldots, k_0)\ ) = 0$ теңдеуін қарастырамыз.

Бірінші шартқа назар аударсақ. Бізде $hg = t$; теңдікті h-қа көбейте отырып, $hg = th$-ты аламыз. Демек, $t = th$, немесе $(h \oplus 1)t = 0$. Бірінші жағдайға байланысты келесіні аламыз:

1) $(h(x)\oplus 1)t(x) \equiv 0$ болатын $t \not\equiv 0$ шағын дәрежедегі функция бар.

Осылайша, h функциялы фильтрлаушы генераторының алгебралық криптоталдауына кедергі келтіру үшін, барлық g функциялардың, $hg = 0$ немесе $(h \oplus 1)g = 0$ болатындай, $\deg(g)$ алгебралық дәрежесі барынша үлкен болуы керек. h функциясының алгебралық иммунитеті деп осындай g функцияларының минималды дәрежесі аталады.

Бастапқы нәтижелер және сызықсыздықпен байланыс

$\deg(f)$ дәрежесі функцияның алгебралық иммунитетінің табиғи жоғарғы бағасы екенін көруге болады. Сонымен қатар, алгебралық иммунитеттің келесі жоғарғы шегі айнымалы n санына байланысты ғана екені белгілі.

Теорема (AI-нің жоғарғы бағалауы). Еркін айнымалылардың f булевтік функциясы үшін бізде $\mathrm{AI}(f) \leq \lceil n/2 \rceil$ орындалады, мұнда $\lceil k \rceil$ – k санының үстіндегі бүтін бөлік.

Бұл бағалау келесі теоремалардағы мысалдармен расталады.

Теорема (максималды AI функциясы). n айнымалылардың келесі функциялары максималды алгебралық иммунитетке ие $\lceil n/2 \rceil$:

1) тақ үшін n: $f(x) = \begin{cases} 0, & \text{егер } \mathrm{wt(x)} < \lceil \mathrm{n/2} \rceil, \\ 1, & \text{егер } \mathrm{wt(x)} \geq \lceil \mathrm{n/2} \rceil. \end{cases}$

2) жұп үшін n: $f(x) = \begin{cases} 0, & \text{егер } \mathrm{wt(x)} < \mathrm{n/2}, \\ \mathrm{b} \in \{0,1\}, & \text{егер } \mathrm{wt(x)} = \mathrm{n/2}, \\ 1, & \text{егер } \mathrm{wt(x)} > \mathrm{n/2}. \end{cases}$

Максималды алгебралық иммунитетті функцияның мысалдары бар болса да, осы функциялар класы туралы ақпарат өте аз. Сондай-ақ, ерікті функцияның алгебралық иммунитеті өте жоғары екендігін көрсетеді.

Теорема (AI кездейсоқ функциясы). Кез келген $a < 1$ және барлық n айнымалылардың f булевтік функциялары үшін, бізде $\mathrm{AI}(f) > n/2 - \sqrt{\mathrm{n}/2 \cdot \ln(\mathrm{n}/(2\mathrm{a}\ln 2))}$ орындалады.

Теорема (AI және N_f байланысы). n айнымалылардың f булевтік функциялары үшін келесі теңдік орындалады: $N_f > 2\sum_{\mathrm{i}=0}^{\mathrm{AI(f)}-2} \mathrm{C}_{n-1}^{i}$.

Осы бағалауға сәйкес, сызықсыздық пен функцияның алгебралық иммунитетінің тәртібі «бір-біріне қайшы келмейді», жоғары алгебралық иммунитет жоғары сызықсыздыққа кепілдік бермейді. Шынында да, оңтайлы алгебралық иммунитет кезінде $\lceil n/2 \rceil$, бағалау мынадай түрде болады: n тақ кезінде $N_f \geq 2^{n-1} - \mathrm{C}_{n-1}^{(\mathrm{n}-1)/2}$ және n жұп кезінде $N_f \geq 2^{n-1} - \mathrm{C}_{n}^{\mathrm{n}/2}$.

4 AES, ГОСТ 34.12-2015, СТБ 34.101.31-2011 ауыстыру блоктарының криптографиялық қасиеттерін салыстырмалы талдау

AES - Advanced Encryption Standard

Қазіргі уақытта АҚШ-та қабылданған және стандартталған Advanced Encryption Standard (AES) алгоритмі пайдаланылады. Бұл стандарт симметриялы шифрлау үшін ең көп таралған алгоритмдердің бірі.

AES – 128 битті деректер блогын шифрлау және шифрін кері ашу үшін қолданады. Стандартта 128 бит, 192 бит және 256 битті ұзындықтағы кілттер пайдаланылады.

AES-та сызықсыз түрлендіруді, әр раунда орындалатын 4 ауыстырудың ішіндегі SubBytes орындайды, яғни S-блокта байттық ауыстыру кестесі.

S-Box (ауыстыру кестесі) - бір байтты басқасына кескіндеуді анықтайтын блок (биективті кескіндеу) [А.4.1-кесте].

Ауыстыру кестесінің кері кестесі - S-Box сияқты, кері кескіндеуді орындайды [А.4.2-кесте]

AES соңғы өрістегі мультипликативті инверсияға негізделген S-блокты қолданады. Ауыстыру блогы кездейсоқтыққа жақын болып келеді. Яғни, барынша кездейсоқ алынған блоктың криптотұрақтылығы жоғары болады. Ауыстыру түйіндерін генерациялау математикалық амалдарға негізделіп жасалады.

S-блоктың элементі неге тең екенін білу үшін бізге келесі үш іс-әрекетті орындау қажет:

1. GF (2^8) өрісінде b-ға кері байтты табыңыз (нөлді өзгеріссіз қалдырамыз). Яғни, кез-келген нөлден басқа b байтында, $a = b^{-1}$ кері байты бар және де $a \bullet b = \{01\}$ қасиетіне ие.

2. Сегіз биттен тұратын нәтижені 64 биттің 8 × 8 матрицасы бойынша көбейтеміз.

3. {63}-ті қосамыз.

Осы орындалған үш іс әрекет афинды түрлендіруді береді.

Биттен құралған матрица қалай құрылғанын түсіну қиын емес. Көбейту үшін «and» операциясын, ал қосу үшін «xor» операциясын қолдану қажет. Бұл жерде кері байтты алу үшін Евклидтің кеңейтілген алгоритмі қолданылады.

Стандартта SubBytes сызықсыз түрлендіруі дифференциалды шабуылға тұрақтылықты арттырады. Кіріс және шығыс айырмашылықтарының сәйкестігіне байланысты, кірісте ΔA айырмашылығына байланысты, шығыста қандай ықтималдылықпен ΔC айырмашылығын көрсететіні негізгі қасиеттері ретінде анықталып отыр. Кіріс және шығыс

айырмашылықтарының тәуелділіктер кестесі өте үлкен көлемге ие: 256 қатар мен 256 бағандар, себебі SubBytes түрлендіру бүкіл байтты ауыстырады.

Бізге ауыстыру блогының негізгі 4 қасиеті төменде келтірілген:

1. Кестедегі ең үлкен мән - бірінші ұяшықты қоспағанда 4-ке тең, $\Delta A=0$ және $\Delta C = 0$ айырмашылығына сәйкес келетін мәні 256-ға тең.

2. Әрбір кіріс айырмашылығы үшін тек бір шығу айырмасы p = 4/256 ықтималдықпен кездеседі, қалған барлық шығу айырмашылықтары p = 2/256 пайда болу ықтималдығына ие.

3. Шығыстағы нөлдік айырмашылық, кірісте нөлдік айырмашылық болғанда ғана кездеседі. DES шифрлау алгоритмінен айырмашылығы шығыстағы нөлдік айырмашылық кірістегі нөлдік емес айырмашылық кезінде де жиі кездесетіндігінде.

4. ΔA = 197 кіріс айырмашылығының мәні p = 4/256 ықтималдықпен шығу кезінде өзгеріссіз қалады, қалған кіріс айырмашылықтары өзгермейді немесе екі есе аз ықтималдылыққа ие.

Аталған қасиеттердің бірінші және екінші бөліктерінде, шығу айырмашылығының біркелкі бөлінуі көрсетіледі, бұл криптоаналитиктердің жұмысын едәуір қиындатады. Үшінші қасиетте айырмашылықтарды қолданғанда, SubBytes-ты түрлендіруін пайдаланғаннан кейін, нөлдік емес айырмашылықта, оның орнына нөлге тең айырмашылық болады. Мұндай өзгерістер DES алгоритмін талдау кезінде кеңінен қолданылады. Әлбетте, Rijndael алгоритмі авторлары бұрынғы шифрлау стандартының осы әлсіз жағын ескеріп, жаңа стандартты криптоталдауға тұрақты етіп шығарған.

ГОСТ Р 34.12-2015 стандарты

Ресейде ГОСТ Р 34.12-2015 шифрлау алгоритмі қолданылады. Бұл стандарт «Магма» деп аталатын ГОСТ 28147-89 стандартының орнына келген.

Бұл стандартта блок ұзындығы n = 128 бит және n = 64 битті, кілт ұзындығы k = 256 битке тең екі негізгі блоктық шифры сипатталған.

Осы стандартта блок ұзындығы n = 128 битпен сипатталған шифр «Кузнечик» («Kuznyechik») блоктық шифры деп аталады.

Осы стандартта блок ұзындығы n = 64 битпен сипатталған шифр «Магма» («Magma») блоктық шифры деп аталады .

Шифрлау бірнеше ұқсас раундтарды тізбектерді қолдануға негізделеді, олардың әрқайсысында үш түрлендіргіш бар: $\boldsymbol{X}$ – раундық кілтпен қосу, $\boldsymbol{S}$ – ауыстыру блогымен түрлендіру, $\boldsymbol{L}$ – сызықтық түрлендіру.

Ұзындығы n = 128 битті блоктық шифрлау үшін биективті ауыстыру сызықты емес түрлендіру ретінде пайдаланылатын келесі массив ретінде беріледі: $\pi' = (\pi'(0), \pi'(1), \dots, \pi'(255))$.

π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101,90, 226, 92, 239, 33, 129, 28, 60, 66 , 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6 , 11,237, 152, 127, 212, 211,31,235, 52, 44, 81,234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8 , 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141,83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91,203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).

Ұзындығы n = 64 битті блоктық шифрлау үшін биективті ауыстыру сызықты емес түрлендіру ретінде пайдаланылатын келесі массив ретінде беріледі: π' = (π'(0), π'(1), … , π'(255)) [А.4.3-кесте].

ГОСТ алгоритмінің стандартына сәйкес, №4.3-кестеде ауыстыру блоктарының жиынтығы берілген. Осы интерпретацияға сәйкес (стандартта бұл блок π деп белгіленген және 0-ден басталады), S1 блогы ең төменгі байтқа, ал S8 деректер блогының ең жоғары байтына қолданады.

Стандартта берілген ауыстыру блоктарының кейбір кірісі, S-блоктан өткеннен кейін өзгеріссіз қалып отырады және кестеде сары түспен көрсетілген.

Егер алмастыру блогындағы кіріс айырмасы нөлдік айырмашылыққа ие болса (яғни, айырмашылықты білдіретін мәтіндер бірдей), онда осы түрлендірудің шығуында айырмашылық нөлдік мәнге ие болады. Егер кіріс айырмашылығы нөлге тең емес болса, онда ол кейбір ықтималдықтармен әртүрлі мәндерге түрлендірілуі мүмкін. Жалпы алғанда, кіріс және шығыс айырмашылықтарының сәйкестігін анықтау алгоритмі төмендегідей болуы мүмкін:

Ауыстыру блогын талдау алгоритмі

1. Ауыстыру блогы анықталып, оның кірісі n биттерді қабылдайды.

2. Осы ауыстыру блогы үшін талдау кестесінде барлық бастапқы мәндер 0-ге тең болады.

3. ΔA = 0 кіріс айырмашылығының бірінші ықтимал мәні анықталады.

4. Талданатын S-блоктағы алғашқы кірістің мәні X = 0 анықталады.

5. X’ = X⊕ΔA кірісінің екінші мәні есептеледі.

6. X және X’ кірістері үшін, S-блоктың жұмыс принципі бойынша, Y және Y’ шығыстары тиісті түрде анықталады.

7. Шығыс айырмашылығының мәні есептеледі $\Delta C = Y \oplus Y'$.

8. Талдау кестесінде, ΔA қатарының саны мен ΔC бағанының санының қиылысында тұрған мән 1-ге дейін артады.

9. X шамасы 1-ге көбейеді.

10. Егер $X < 2^n$, онда 5-қадамға өтеді.

11. ΔA шамасы 1-ге көбейеді.

12. $\Delta A < 2^n$ болса, 4-қадамға өтеді.

13. Егер барлық ауыстыру блоктары талданса, онда 1-қадамға көшу орын алады, әйтпесе алгоритм өзінің жұмысын аяқтайды.

S-блокты талдау алгоритмін қолдану нәтижесінде №1 кестеде келтірілген әрбір S-блоктарының дифференциалдық тәуелділіктерін көрсететін сегіз кесте алынды. Жасалған кестелерді талдау келесі заңдылықтарға негіз болды:

1. Бір көлденең сызықтың барлық мәндерінің сомасы, яғни ΔA кіріс айырмашылығының бірдей мәніне сәйкес келетін шығу коэффициенттерінің әр түрлі мәндерінің саны әрқашан 2^4-ке тең.

2. Кіру айырмашылығының ΔA нөлден тыс мәні блоктарының біреуінде ΔC = 0 мәніне алмастырылмайды.

3. Талдау кестелерінде 1/4 артық емес ықтималдығы бар айырмашылық жұптары жоқ (ΔA, ΔC).

4. S1 ауыстыру блогы үшін:

− ΔA = 14 кіріс айырмашылығы ΔC айырмашылықтарына әкеледі, онда жоғары бит әрдайым 0-ге тең болады;

− кіру айырмашылықтары ΔA = 5 және ΔA = 11, ΔC айырмашылықтарына әкеледі, онда ең жоғарғы бит әрдайым 1-ге тең болады.

5. S2 ауыстыру блогы үшін:

− ΔA = 8 кіріс айырмасы ΔC айырмашылықтарына алып келеді, онда жоғары бит әрдайым 0-ге тең болады;

− ΔA = 7 және ΔA = 15 кіріс айырмашылықтар ΔC айырмашылықтарына әкеледі, онда ең жоғары бит әрдайым 1-ге тең болады.

6. S5 ауыстыру блогы үшін:

− ΔA = 8 кіріс айырмашылығы ΔC айырмашылықтарына алып келеді, онда жоғары бит әрдайым 0-ге тең болады;

− кіру айырмашылықтары ΔA = 1 және ΔA = 9, ΔC айырмашылықтарына әкеледі, онда ең жоғарғы бит әрдайым 1-ге тең болады.

7. S6 ауыстыру блогы үшін:

− ΔA = 9 кіріс айырмашылығы ΔC айырмашылықтарына әкеледі, онда төмен бит әрдайым 0-ге тең болады;

− ΔA = 14 кіріс айырмашылығы ΔC айырмашылықтарына әкеледі, онда төмен бит әрдайым 1-ге тең болады;

8. S7 ауыстыру блогы үшін:

− ΔA = 13 кіріс айырмашылығы ΔC айырмашылықтарына әкеледі, онда жоғары бит әрдайым 0-ге тең болады;

− ΔA = 3 және ΔA = 14 кіріс айырмашылықтары ΔC айырмашылығына әкеледі, онда ең жоғарғы бит әрдайым 1-ге тең болады.

Анықталған заңдылықтар үлкен қызығушылық тудырады және кейінірек мүмкін емес дифференциалдарға арналған іздеу алгоритмін әзірлеуде қолданылатын болады.

СТБ 34.101. 31-2011 Беларустық стандарты

Осы стандарт деректердің құпиялылығын қамтамасыз етуге және тұтастығын бақылауға арналған криптографиялық алгоритмдер отбасын анықтайды. Өңделетін деректер екілік сөздер (хабарлар) болып табылады.

Стандартты криптографиялық алгоритмдер деректер блогын шифрлаудың базалық алгоритмдері негізінде құрылған. СТБ 34.101. 31-2011-256 биттік кілтпен және 128 биттік сөздермен операция жасайтын 8 криптотүрлендіргішті циклмен құрылған блоктық шифр.

Сызықсыз түрлендіру ретінде келесі түрдегі ауыстыру блоктары қолданылады: $\{0, 1\}^8 \rightarrow \{0, 1\}^8$ [А.4.4-кесте] келтірілген.

S-блоктың криптографиялық қасиеттері алгоритмнің қауіпсіздігінде маңызды рөл ойнайды, себебі осы түйіндер ғана сызықсыздықты қамтамасыз етеді. Құрастырушылар ауыстыру түйіндерін генерациялағанда, ол қалай құрылғанын, S-блок қандай конструкцияға ие және неге оны қолданғанын түсіндіру керек. Мысалы AES соңғы GF(28) өрісте мультипликативті терістеуге негізделген S-блокқа ие.

Ауыстыру түйіндерінің генерациялануының құпия болуы жақсы немесе жаман екені жайында көптеген бәсекелестіктер тууда. Бір жағынан алдын-ала тексерілген және қалыптастырылған ауыстыру блоктары шифрлау алогитміне жоғарғы тұрақтылықты беруі тиіс. Екінші жағынан егер блоктар құпия болса алгоритмге кездейсоқтығымен қатар үлкен сенімділік беруі керек.

Белорустық BelT шифрінің S-блоктарының генерациялау алгоритмі Кузнечик шифрмен ұқсас екені дәлелденген. Яғни, олар құпия түрде сақталынған. «CRYPTO 2015» конференциясында Алекс Бирюков, Лео Перрин және Алексей Удовенко кері жобалау тәсілімен, жасырын алгоритммен генерацияланған S-блокты, құрушылардың мәлімдемесіне

қарамастан, Кузнечиктің ауыстыру түйіндері жалған кездейсоқ емес екенін дәлелдеген. Бұдан байқайтынымыз алгоритм қанша жасырын болғанымен, ауыстыру түйіндері жалған кездейсоқ болмаса, S-блоктың криптографиялық қасиеті нашар екенін көрсетеді.

Осы ауыстыру блоктарының криптографиялық қасиеттері төменгі 4.5-кестеде көрсетілген:

Қасиеті	Мағынасы		
	AES	СТБ	ГОСТ
Булевтік функция қасиеттері			
Теңестірілген	Иә	Иә	Иә
Сызықсыздық	112	102	104
$\|AC\|_{max}$	32	88	88
Минималды дәреже	7	7	7
AI	2	3	3

5 Криптографиялық тұрақты векторлық булевтік функцияны генерациялау әдістері

Кез-келген блоктық шифрлар үшін ауыстыру блоктарының дифференциалды криптоанализге тұрақты болуын жобалаудың бірқатар белгілі критерилері бар:

– қаттаң лавинды эффектілік критериі (Strict Avalanche Criterion, SAC) кез келген i және j үшін, ауыстыру түйінінің кірісінде i битін өзгерткенде, шығыс битінің ықтималдығы 0,5-ке өзгереді;

– биттердің тәуелсіздік критериі (Bit Independence Criterion, BIC) кез-келген i, j және k мәндерінде кіріс битін ауыстыру түйінінің кірісіне енгізу кезінде, j және k шығу биттері өздігінен өзгереді, яғни бір мезгілде биттерді өзгерту ықтималдығы жеке биттерді өзгерту ықтималдығы туындысына тең болу керек. SAC және BIC критерийлерінің барлық ауыстыру түйіндерінде бір уақытта орындалуы шифрдың лавинды әсерінің жеткілікті деңгейіне жетуіне кепілдік береді;

– кепілденген лавиндық әсер критериі (GAC) ауыстыру түйінінің кірісінде кемінде бір биттің өзгеруі шығысында кемінде g шығыс биттерінің өзгеруіне алып келеді. Ауыстыру блокатары үшін g ретті 2-ден 5-ке дейінгі диапазон аралығындағы GAC критериінің орындалуы раундтық шифрлауда Фейстель желісі арқылы өтуде биттердің өзгеруінің таралуына байланысты шифрға өте үлкен лавинды эффектіні береді.

Ауыстыру түйіндерін генерациялаудың, яғни таңдаудың көптеген кең таралған тәсілдері бар:

– кездейсоқ таңдау, кездейсоқ сандардың генераторын пайдалана отырып, ауыстыру түйіндерінің элементтерін таңдау. Алайда бұл ГОСТ 28147-89 алгоритмінде (4x4 бит) кішкентай ауыстыру түйіндер жағдайында қолданылатын ең жеңіл әдіс болып табылады. Бұл әдіс шифрдың сызықсыздық пен лавиндық әсер сипаттамалары бар ауыстыру түйіндерінің генерациялануына алып келуі мүмкін;

– кейіннен тексеру арқылы кездейсоқ таңдау. Бұл әдісте ауыстыру түйіндерінің элементтері кездейсоқ түрде таңдалады, бірақ кейін алынған нәтижелер әртүрлі критерийлерге сәйкестігіне байланысты тексеріледі және критериге сәйкес емес түйіндер қысқартылады. Бұл әдіс бірінші әдіс сияқты қарапайым, сонымен қатар бірінші әдістің кемшілігін жояды. Барлық критериге сәйкес келетін ауыстыру түйіндерін құру мүмкін емес;

– қолмен іріктеу, ауыстыру түйіндерінің элементтері математикалық түрлендірулер арқылы қолмен таңдалады. Бұл әдіс DES алгоритмінде оның тұрақты S-блоктарын әзірлеу үшін негіз болды. Мұндай тәсіл күрделі

әдістердің бірі болып табылады, өйткені ол әрқашан мүмкін бола бермейтін ауыстырғыштарды таңдау әдісін әзірлеуді және теориялық негіздеуді талап етеді;

– ауыстыру түйіндерінің элементтері белгілі бір математикалық қағидаларға негізделген нақты алгоритм көмегімен қалыптастырылған математикалық тәсіл. Бұл әдіс сызықтық және дифференциалды криптоанализ әдістеріне қатысты сенімділіктің белгілі бір деңгейіне кепілдік беретін ауыстыру түйіндерін таңдауға мүмкіндік береді.

Блоктық шифрларда ауыстыру түйіндеріне (S-блоктарға) қойылатын жалпы талаптар, шифрлау функцияларына қойылатын талаптарға сәйкес келеді, яғни сызықсыздық пен лавинды эффекттің болуы.

f функциясының сызықсыздығы келесі формуламен анықталады:

$$nl(f) = min_{l \in A_4} wt(f \oplus \mathrm{l}),$$

мұнда *wt* – Хэммингa салмағы функциясы (функция шығу кезінде 1 мәнін беретін әр түрлі кіріс бит комбинацияларының саны); A4 – 4 айнымалылардан тұратын аффинді булевтік функциясы (сызықтық функциялар және олардың биттік инверсиялары).

S ауыстыру түйіндерінің сызықсыздығы келесі түрде келтіріледі:

$$nl(S) = min_{l \in C} nl(f),$$

мұнда C – $C = \{Mc, c \in \{0,1\}^4\}$ ауыстыру түйіндерінің 16x4 өлшемді биттік M матрицасының бағанының барлық сызықты комбинация жиынтығы. M матрицасының векторға туындысы екілік модуль бойынша есептеледі.

Осылайша, ауыстыру түйінінің сызықтық емес талабы мынадай түрде тұжырымдалуы мүмкін: түйіннің бит матрицасының бағандарының барлық сызықтық комбинациясы, $nl(f) = min_{l \in A_4} wt(f \oplus \mathrm{l})$ формуласымен анықталатын ең үлкен сызықсыздыққа ие болуы керек. 4 айнымалыдан булевтік функцияны толықтай іріктегенде, бағанның сызықсыздығы тек 0, 2 және 4 мәндерін қабылдауы мүмкін екендігі анықталды.

Ауыстыру түйінімен қамтамасыз етілетін лавинды әсерінің дәрежесі, j ретті матрицаның динамикалық қашықтығымен сипатталады:

$$\mathrm{DD}_j(f) = max_{\substack{d \in \{0,1\}^4 \\ 1 \le wt(d) \le j}} \frac{1}{2} \left| 2^{n-1} - \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus d \right|$$

Сонда (i, j)-ретті S ауыстыру блогының динамикалық қашықтығы келесі түрде анықталады

$$\mathrm{DD}_{i,j}(S) = max_{\substack{c \in \{0,1\}^4 \\ 1 \le wt(c) \le i}} \mathrm{DD}_j(Mc),$$

мұнда M – ауыстыру блогының биттік матрицасы.

Осылайша S ауыстырушы түйініне арналған SAC критериі $\mathrm{DD}_{1,1}(S) = 0$, немесе, биттік матрицаның S бағанының барлық бағандары 1-ретті 0-ге тең

динамикалық қашықтыққа ие болған жағдайда ғана қанағаттандырылады және BIC критерийі $DD_{2,1}(S) = 0$ болған кезде жүзеге асырылады, яғни ауыстыру түйіндерінің S биттік матрицасының барлық жұп бағандарының сызықтық комбинациясы 1-ретті, 0-ге тең динамикалық қашықтыққа ие.

Осылайша, ауыстыру түйініне лавинды әсерін қамтамасыз ету талабы келесі түрде тұжырымдалуы мүмкін: түйіннің бит матрицасының бағандарының барлық сызықтық комбинациясы барынша мүмкін болатын ең қысқа динамикалық қашықтыққа ие болуы қажет.

Ауыстыру блоктарын құрудың келесі алгоритмі, ауыстыру түйіндерін этап, баған бойынша құруды ұсынады:

1-қадам. Сызықсыздықтың минималды рұқсат етілген дәрежесі nl_{min} мәні және ауыстыру түйінінің бит матрицасы бағандарының сызықтық комбинациясы 1 DD_{max} тәртібінің рұқсат етілген ең жоғары динамикалық қашықтығы таңдалады;

2-қадам. 4 айнымалылардан булевтік функциясының барлық мүмкін 2^{16}=65536 ішкі жиынынан 1-қадамда таңдалған критерийлерді қанағаттандыратын толық іріктеу әдісімен таңдалады;

3-қадам. 2-қадамда жасалған ішкі жиыннан «кандидат» функциясы таңдалады және ауыстыру түйінінің биттік матрицасының бірінші бағанына орналастырылады;

4-қадам. 2-қадамда жасалған ішкі жиыннан «кандидат» функциясы таңдалады және бит матрицасының екінші бағанына орналастырылады, содан кейін бірінші және екінші бағандардың екілік модуль бойынша суммасы 1-қадамда таңдалған критерийлерге сәйкес тексеріледі. Егер бұл функция оларды қанағаттандырмаса , екінші бағанда орналасқан функция алынып тасталады және 3-қадамға оралады;

5-қадам. «Кандидат» функциялары 2-қадамда жасалған және бит матрицасының бағандарында соңғы толтырылған бағаннан кейін таңдалған ішкі жиындардан таңдалады, содан кейін матрицаның барлық 4 бағандары толтырылмайынша, бағандардың барлық сызықтық комбинацияларында «кандидат» бағанымен тексерулер орындалады;

6-қадам. Ауыстыру түйінінің нәтижесінде алынған бит матрицасы GAC-ге сәйкестігі үшін, сондай-ақ ауыстыру түйінінің XOR-кестесін құрастыру арқылы дифференциалды криптоанализге қарсылық үшін тексеріледі. Егер осы критерийлер орындалса, ауыстырушы түйін алгоритмнің шығуына айналады, егер орындалмаса, бит матрицасының соңғы бағанынан бас тартылады және процесс 5-қадамға қайтарылады, яғни «кандидатты» тестілеу процесі жалғасады.

6 Векторлық булевтік функцияны генерациялау және криптографиялық қасиеттерін зерттеу

Ауыстыру түйіндерін бір уақытта оптималды криптографиялық көрсеткіштерімен генерациялау теориялық және тәжірбие жүзінде іске асыру күрделі тапсырмалардың бірі. Сызықсыз ауыстыру түйіндерін генерациялауда алғашында тиімді S-блоктарды табу үшін n = m = 6 мәні қолданылған. Заманауи блоктық симметриялық шифраларда оптималды ауыстыру түйіндерін алу үшін n = 8 мәні пайдаланылады.

Яғни, n = 8 тиімді ауыстыру блоктарын табу үшін келесі көрсеткіштерге ие болу керек:

– минималды дәреже 7;

– алгебралық иммунитет 3;

– 8-теңестірілген;

– сызықсыздық 104;

Келесі көрсетілген тәсілдермен бізге оптималды ауыстыру тізбектерін алуға болады:

– булевтік функция орнына векторлы булевті функцияны қолдану керек.

– бент-функция орнына максималды көрсеткішті теңдік пен сызықсыздықты булевтік функцияны алу қажет.

Осы тәсілдер арқылы *NP* мәнін (1-ден бастап) үлкейткенде, бізге тәжірбиелік жолмен ауыстырудың барлық қасиеттеріне ие *NP=22* мәні табылды. Осы ауыстыру түйіндері келесі 6.1-кестеде, ал криптографиялық қасиеттері 6.2-кестеде келтірілген:

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	c4	ca	ff	b1	be	2c	6f	c2	aa	62	3f	84	2b	f0	5c	30
1	86	a5	6b	da	bf	31	4b	40	52	3b	02	79	27	ea	ba	61
2	bd	69	44	63	0c	72	b0	1a	3c	70	76	e7	cb	19	14	c8
3	7b	22	11	8b	99	9b	b9	20	92	fc	7a	6a	dd	d0	4c	eb
4	74	c1	53	d5	ae	ab	09	34	c0	f1	59	b8	57	f5	d4	db
5	95	1d	15	a3	e8	a1	d9	c5	88	67	39	a2	e1	96	f2	37
6	a0	41	fb	47	cc	46	4d	56	8d	3a	a6	fe	4a	bb	04	b4
7	d8	94	ad	87	75	33	83	de	68	06	51	18	0e	bc	a4	e4
8	f9	64	e3	85	8e	66	f7	d3	b5	cf	32	f8	60	ce	17	ed
9	7f	49	8f	4e	5f	e5	e9	1e	b7	0a	7c	4f	a9	0d	c7	0f
a	b6	77	01	5e	13	d1	af	91	9d	36	2a	48	58	a7	5b	fd
b	d7	d6	16	5d	93	1b	98	80	dc	c3	7e	cd	2f	3e	03	f3
c	54	6c	0b	b3	35	e0	38	e6	c9	ec	5a	7d	73	21	9a	25
d	f6	c6	42	90	6e	12	07	8a	8c	df	9f	82	29	81	89	ee
e	1c	00	28	05	2e	10	26	43	08	65	9c	9e	78	fa	3d	45
f	ef	ac	a8	71	50	1f	97	2d	24	6d	b2	55	e2	23	d2	f4

6.1-кесте. Жоғарыда келтірілген алгоритм бойынша генерацияланған оптималды ауыстыру кестесі

Қасиеті	Мағынасы
Булевтік функция қасиеттері	
Теңестірілген	Иә
Сызықсыздық	102
$\|AC\|_{max}$	88
Минималды дәреже	7
AI	3

6.2-кесте. 6.1-кестедегі ауыстыру түйіндерінің криптографиялық қасиеттері

Бұл ауыстыру түйіндерін генерациялау «Sage» компьютерлік алгебра жүйесінде жасалған. Осы жүйе бойынша генерацияланған ауыстыру блоктары криптографиялық қасиеттеріне байланысты әр түрлі құрылымға ие. Бағдарламалық қамтаманы пайдалану арқылы сызықсыздығы 102-ден жоғары ауыстыру блоктары алгебралық иммунитеті жағынан оптималды болмай шықты. Бірақ та сызықсыздығы 104-ке тең, ал алгебралық иммунитеті 2-ге тең ауыстыру түйіндері де генерация нәтижесінде табылды. Осы ауыстыру блоктары және оның сипаттамалары сәйкесінше 6.3-ші, 6.4-кестелерде келтірілген.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	49	95	69	a4	2c	e7	ef	d8	b8	8b	6c	1e	be	30	5f	04
1	42	cf	e1	1f	c2	a5	cc	ff	84	af	bd	2b	b0	3f	dd	78
2	b9	39	37	c7	77	61	f2	72	c5	8d	b1	47	4f	52	7b	bc
3	89	ac	79	7e	ba	44	12	e8	74	93	34	9b	97	f9	29	10
4	eb	5d	96	d1	85	bb	b6	cd	6f	75	ad	8a	8e	ee	ed	f5
5	c3	9c	19	3b	c0	2a	5a	62	b7	07	87	06	b3	60	54	c1
6	31	86	d2	1d	76	28	43	e4	27	66	b5	6d	a1	f1	e9	0f
7	4e	e0	08	2f	cb	55	45	fd	81	f0	d7	68	ec	0d	6a	82
8	26	00	0b	05	7a	3c	09	e2	a9	3e	fc	21	33	b4	71	ca
9	9e	1a	90	1c	a8	8f	83	91	46	b2	fb	94	c4	64	6e	13
a	f6	51	a0	bf	6b	a7	0a	c6	db	20	59	9d	d3	58	a3	a6
b	92	a2	d6	5e	aa	56	da	38	03	7c	63	ab	18	14	25	70
c	23	ae	32	57	80	e5	53	fe	f8	50	3a	35	e6	d4	4d	d5
d	c8	02	41	4b	df	ce	40	01	65	7f	de	7d	fa	d9	16	e3
e	9a	2e	4a	98	15	24	88	ea	2d	f4	99	d0	36	67	4c	0c
f	22	17	f7	11	c9	f3	5c	8c	48	73	3d	1b	9f	5b	dc	0e

6.3-кесте Теңсіздіктер саны аз және алгебралық иммунитеті 2-ге тең ауыстыру блогы

Қасиеті	Мағынасы
Булевтік функция қасиеттері	
Теңестірілген	Иә
Сызықсыздық	104
$\|AC\|_{max}$	80

Минималды дәреже	7
AI	2
Корреляциялық иммунитет	0
Қатаң лавинды сиппаттама	Жоқ

6.4-кесте. 6.3-кестедегі ауыстыру түйіндерінің криптографиялық қасиеттері

«Sage» компьютерлік алгебра жүйесінде оптималды ауыстыру блоктарын алу үшін, көптеген есептеулер жүргізу қажет. Және де келесі 6.5-ші, 6.6-кестелерде сызықсыздығы 104-ке тең, ал алгебралық иммунитеті 3-ке тең ауыстыру түйіндері келтірілген.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	ab	99	2a	0d	1a	6c	90	c3	65	4a	d1	e5	36	95	b3	ff
1	e1	43	19	53	1c	6d	ec	fe	60	17	fa	5d	05	4d	ea	b1
2	50	d0	92	40	ee	9c	22	4c	b9	88	07	18	68	0f	57	dd
3	ae	a0	aa	7f	5c	02	89	a4	b4	f2	db	f9	64	3f	b7	c1
4	87	3c	0e	a5	bf	1d	06	5f	cf	7a	da	28	d7	d5	bc	93
5	e2	96	9a	ba	dc	7d	ed	9f	d6	32	08	c4	30	c8	61	49
6	91	bd	e6	4e	3d	e9	f7	ac	3e	b2	56	e8	7c	d2	29	2b
7	42	5e	f8	48	ce	26	cd	a8	c6	df	2f	f0	3a	9e	81	4f
8	e3	e7	8d	76	62	34	1e	f3	af	2e	8c	38	51	bb	66	54
9	1f	77	5a	0a	eb	23	fb	3b	70	2c	0c	01	04	4b	ca	13
a	10	41	d8	d4	94	b0	6e	82	39	fc	71	a1	52	b5	58	74
b	31	a9	25	5b	86	97	15	f1	cb	67	f4	27	21	8b	7b	09
c	c7	6b	8a	e0	6f	fd	c2	37	80	a2	ad	be	ef	8f	7e	69
d	a6	c5	16	6a	f6	79	55	98	84	b8	45	35	d3	33	85	78
e	c0	de	9b	59	b6	75	72	9d	f5	03	e4	44	14	cc	1b	a7
f	d9	24	0b	00	11	12	c9	83	73	20	8e	47	46	2d	63	a3

6.5-кесте Сызықсыздығы 104-ке және алгебралық иммунитеті 3-ке тең ауыстыру блогы

Қасиеті	Мағынасы
Булевтік функция қасиеттері	
Теңестірілген	Иә
Сызықсыздық	104
$\|AC\|_{max}$	80
Минималды дәреже	7
AI	3
Корреляциялық иммунитет	0
Қатаң лавинды сиппаттама	Жоқ

6.6-кесте. 6.5-кестедегі ауыстыру түйіндерінің криптографиялық қасиеттері

Бұл зерттеу жұмыстары нәтижесінде қолданылған тәсілдер арқылы оптималды ауыстыру блоктарын алып, оны заманауи блоктық симметриялы

шифрларда қолдануға болады. 6.6-кестеде осы жұмыс нәтижесінде алынған ауыстыру түйіндерінің қасиеттері өзара салыстырылып, айырмашылықтары келтірілген.

Қасиеті	Мағынасы		
	6.1-кесте	6.3-кесте	6.5-кесте
Сызықсыздық	102	104	104
$\|AC\|_{max}$	88	80	80
AI	3	2	3

6.6-кесте. Генерацияланған ауыстыру блоктарының криптографиялық қасиеттері

Кайса Найберг тәсілі бойынша ауыстыру түйіндерін генерациялауды Maple бағдарламалық қамтамасында келтірдік. Генерациялау өрісті терістеу тәсілі бойынша алынды, яғни AES ауыстыру блогын генерациялау тәсіліне сүйенеді. Бағдарлама нәтижесі [Б.6.1-сурет, Б.6.2-сурет, Б.6.3-сурет] қосымшада келтірілген.

ҚОРЫТЫНДЫ

Векторлық булевтық функциялардың математикалық аппаратын пайдалану оңтайлы көрсеткіштермен симметриялық криптографиялық примитивтер үшін сызықты емес орналасу конструкцияларын қалыптастырудың тиімді әдістерін табуға мүмкіндік береді. Бұл вектордың логикалық функциялары шеңберінде әзірленген теориялар шифрдың ұзақ мерзімді негізгі элементтерін құру үшін пайдаланылуы мүмкін. Сызықсыз ауыстыру түйіндерін жылдам генерациялаудың ұсынылған әдісі, криптоталдаулардың танымал түрлеріне айтарлықтай кедергі келтіретін қосымша тұрақтылықты қамтамасыз етеді.

Зерттеу жұмыстары нәтижесінде симметриялы криптоалгоритмдерде қолданылатын ауыстыру түйіндерінің көптеген критерилері талданды. Қазіргі заманғы критерилер криптоталдаудың қолданыстағы түрлерінен: сызықты, алгебралық және түрлі дифференциалдық талдаудан қорғауға бағытталған. Көптеген зерттеулер, сондай-ақ осы жұмыстың шеңберінде ешқандай мінсіз ауыстыру түйіндерін алу мүмкін емес екенін көрсетеді. Осылайша, критерилері нақты шифрлау алгоритмі (немесе алгоритмдер тобы) үшін анықталған және қолданыстағы шабуылдардың түрлерінен қорғау тұрғысынан оңтайлы болып табылатын «оңтайлы ауыстыру» термині енгізілді.

Яғни ауыстыру түйіндерінің қасиеттерін теңестіре отырып оңтайлы блокты генерациялау, шифр алгоритміне қазіргі таңда мүмкін болатын криптоталдауларға қарсы тұруға сенімділігін арттырады.

ҚОЛДАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 ГОСТ Р 34.12 – 2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

2 СТБ 34.101.31 – 2011. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целосности.

3 National Institute of Standards and Technology, «FIPS-197»: Advanced Encryption Standard. Nov.2001.

4 Городилова А.А. Почти совершенно нелинейные функции: характеризация через подфункции и дифференциальная эквивалентность. М. Новосибирск, 2016. –Б. 4–43.

5 Ищукова Е.А. Разработка и исследование алгоритмов анализа стойкости блочных шифров методом дифференциального криптоанализа. М. Таганрог, 2007. –Б. 148–150.

6 Чалкин Т. А., Волощук К. М. Разработка алгоритма построения узлов замен. –Б. 48–50.

7 Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470б.

8 Горбенко І. Д. Прикладна криптологія/ І. Д. Горбенко, Ю. І. Горбенко. – Х. : Форт, 2012. – 870 б.

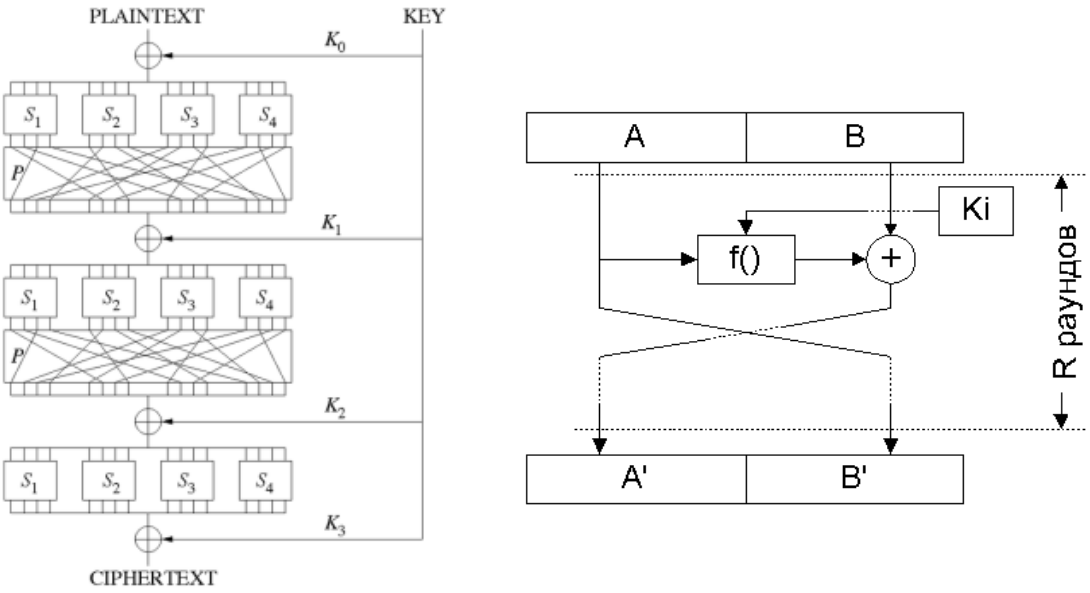
9 Булевы функции в теории кодирования и криптологии / О. Логачев, А. Сальников, С. Смышляев, В. Ященко ; Ин-т проблем информ. безопасности МГУ. – 2-е шығарылым., доп. – М. : МЦНМО, 2012. – 583б.

10 Menezes A. J. Handbook of applied cryptography/ Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – Boca Raton : CRC press, 2010. – 816б.

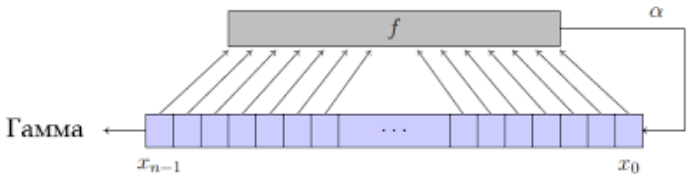
11 ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования – Енг. 01–07–1990. – К. : стандарт баспасы, 1989. – 28б.

12 ДСТУ ГОСТ 28147:2009. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования – Взамен ГОСТ 28147–89 ; енгізілді. 01–02–2009. – К. : стандарт баспасы, 2009.

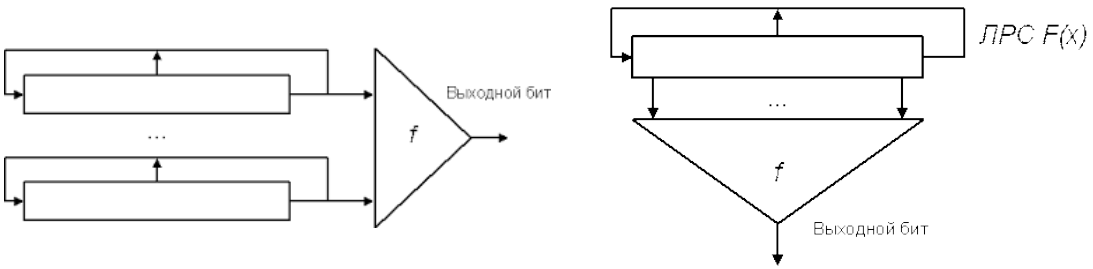
Қосымша А



1.1.1-сурет. SP-желісі және Фейстель желісі



1.4.1-сурет. Кері байланысы бар жылжыту регистрі



1.4.2-сурет. Сызықтық кері байланысы бар жылжу регистрлері негізінде құрылған генераторлар

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

4.1-кесте. AES-тың ауыстыру блогы

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

4.2-кесте. AES-тың кері ауыстыру блогы

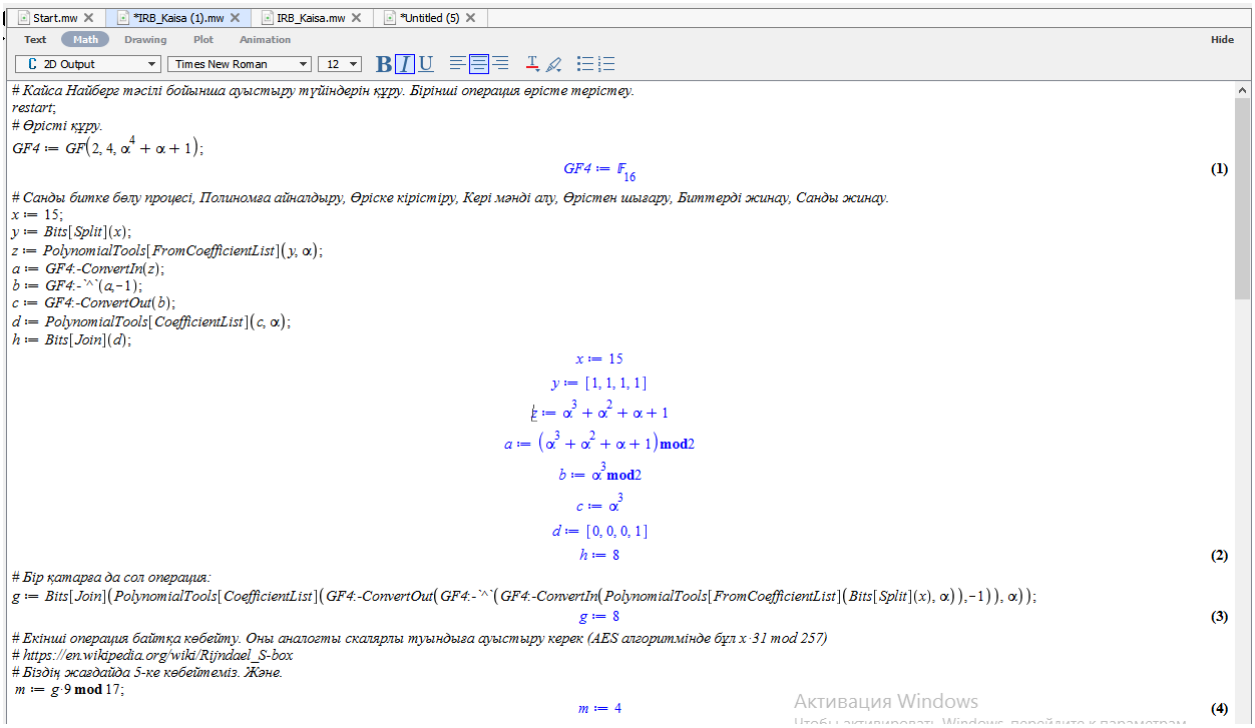
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S1	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
S2	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
S3	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
S4	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
S5	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
S6	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0
S7	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
S8	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

4.3-кесте. Магма ауыстыру блогы

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B1	94	BA	C8	0A	08	F5	3B	36	6D	00	8E	58	4A	5D	E4
1	85	04	FA	9D	1B	B6	C7	AC	25	2E	72	C2	02	FD	CE	0D
2	5B	E3	D6	12	17	B9	61	81	FE	67	86	AD	71	6B	89	0B
3	5C	B0	C0	FF	33	C3	56	B8	35	C4	05	AE	D8	E0	7F	99
4	E1	2B	DC	1A	E2	82	57	EC	70	3F	CC	F0	95	EE	8D	F1
5	C1	AB	76	38	9F	E6	78	CA	F7	C6	F8	60	D5	BB	9C	4F
6	F3	3C	65	7B	63	7C	30	6A	DD	4E	A7	79	9E	B2	3D	31
7	3E	98	B5	6E	27	D3	BC	CF	59	1E	18	1F	4C	5A	B7	93
8	E9	DE	E7	2C	8F	0C	0F	A6	2D	DB	49	F4	6F	73	96	47
9	06	07	53	16	ED	24	7A	37	39	CB	A3	83	03	A9	8B	F6
A	92	BD	9B	1C	E5	D1	41	01	54	45	FB	C9	5E	4D	0E	F2
B	68	20	80	AA	22	7D	64	2F	26	87	F9	34	90	40	55	11
C	BE	32	97	13	43	FC	9A	48	A0	2A	88	5F	19	4B	09	A1
D	7E	CD	A4	D0	15	44	AF	8C	A5	84	50	BF	66	D2	E8	8A
E	A2	D7	46	52	42	A8	DF	B3	69	74	C5	51	EB	23	29	21
F	D4	EF	D9	B4	3A	62	28	75	91	14	10	EA	77	6C	DA	1D

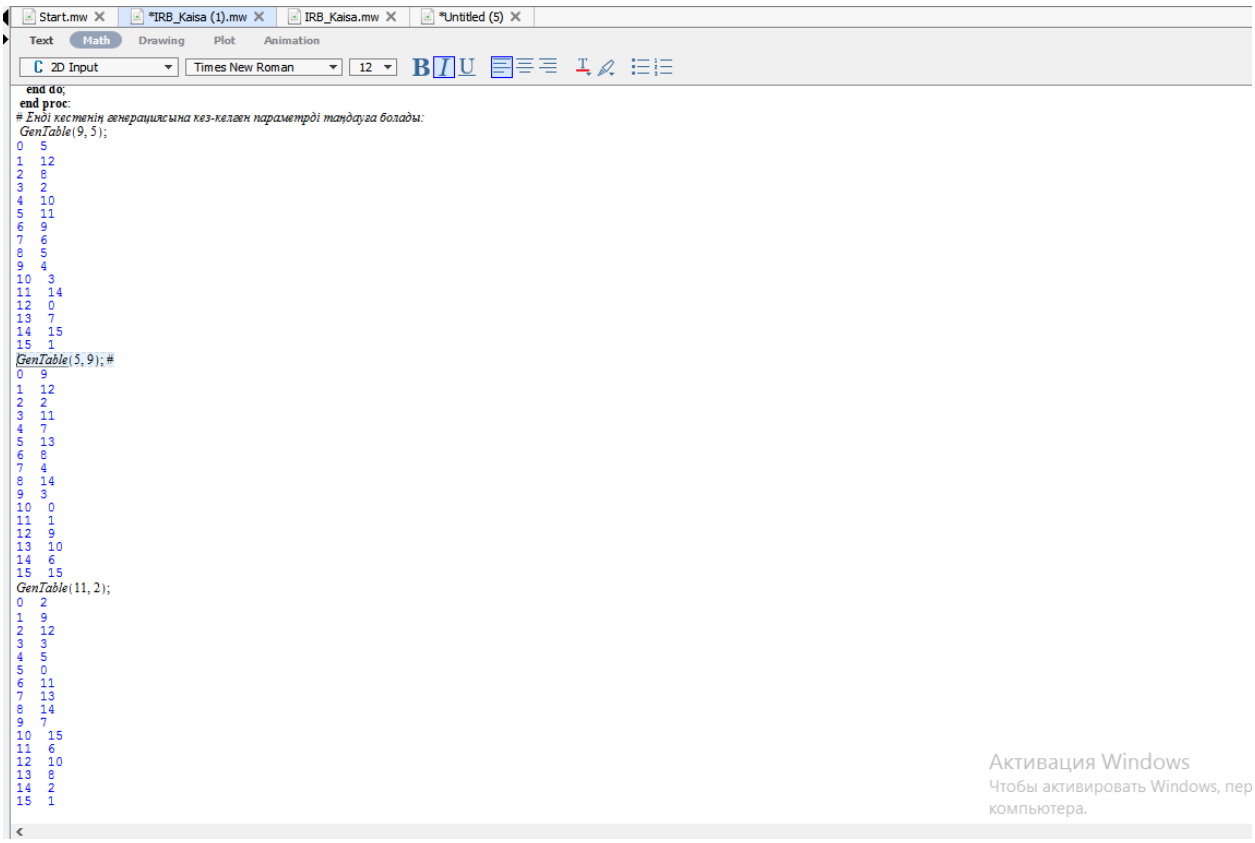
4.4-кесте. СТБ 34.101. 31-2011стандартының ауыстыру блогы

Қосымша Б



6.1-сурет. Генерациялау барысындағы орындалатын операция

6.2-сурет. Генерациялау барысындағы орындалатын операция



6.3-сурет. Генерацияланған ауыстыру түйіндері