ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ТАЪЛИМ, ФАН ВА ИННОВАТSIЯЛАР ВАЗИРЛИГИ
ДЕНОВ ТАДБИРКОРЛИК ВА ПЕДАГОГИКА ИНСТИТУТИ

З.Т.ХУДОЙҚУЛОВ, Э.И.САИДАХМЕДОВ

КРИПТОТАҲЛИЛНИНГ АВТОМАТЛАШГАН ДАСТУРИЙ ВОСИТАЛАРИНИ ИШЛАБ ЧИҚИШ

Термиз–2026

УДК 004.056.55:004.4
КБК 004.056.55
Х-87

З.Т.Худойқулов, Э.И.Саидахмедов
Криптотаҳлилнинг автоматлашган дастурий воситаларини ишлаб чиқиш. // Монография. – “Termiz publishing center” нашриёти, 2026. - 119 б.

Денов тадбиркорлик ва педагогика институти кенгашининг 2026-йил 8 -апрелдаги 7 -сонли байонномасига асосан нашрга тавсийа етилган.

Мазкур монографияда симметрик блокли шифрлаш алгоритмларининг криптобардошлилигини таъминловчи асосий компонент — S-жадваллар (алмаштириш блоклари) нинг математик хоссаларини тадқиқ этиш масалалари ёритилган. Тадқиқот давомида S-блокларнинг чизиқсизлик даражаси, алгебраик иммунитет, лавина эффекти ва баланслашганлик каби муҳим криптографик мезонларини автоматик равишда ҳисоблаш ва баҳолаш имконини берувчи дастурий восита ишлаб чиқилган. Ишда замонавий шифрлаш стандартлари (AES, PRESENT ва ҳ.к.) S-қутиларининг хавфсизлик кўрсаткичлари таҳлил қилинган ва уларни оптималлаштириш бўйича илмий-амалий таклифлар берилган.

Монография ахборот хавфсизлиги ва криптография йўналишида таҳсил олаётган талабалар, магистрлар, мустақил тадқиқотчилар ҳамда соҳа мутахассислари учун мўлжалланган

Масъул муҳаррир:
Шомирзайев Махматмурод Хурамович
Педагогика фанлари доктори, профессор

Тақризчилар:
Р.Я.Мамажанов, Денов тадбиркорлик ва педагогика институти “Ахборот технологиялари” кафедраси т.ф.ф.д. (PhD), доцент.
И.П.Хурамов, Термиз давлат университети Технологик таълим кафедраси ўқитувчиси п.ф.ф.д. (PhD),

ISBN: 978-9910-13-276-6

КИРИШ

Мавзунинг долзарблиги. Инсоният тараққиётининг ҳозирги босқичи жамият ҳаётининг барча соҳаларини жадал рақамлаштириш ва глобал ахборот маконига интеграциялашуви билан тавсифланади. Бугунги кунда давлат бошқаруви, мудофаа тизимлари, стратегик объектлар, молиявий институтлар ва шахсий маълумотлар алмашинуви тўлиқ компьютер тармоқлари ҳамда рақамли платформаларга асосланган. Бундай шароитда ахборот хавфсизлигини таъминлаш нафақат техник масала, балки миллий хавфсизликнинг стратегик устувор йўналишига айланди.

Айниқса, Буюмлар интернети (IoT), сунъий интеллект (AI), катта маълумотлар (Big Data) ва булутли технологияларнинг кенг ёйилиши ҳимояланиши лозим бўлган ахборот ҳажмининг геометрик прогрессияда ўсишига олиб келди. Бундай тизимларда маълумотлар махфийлиги ва бутунлигини таъминлаш учун қўлланиладиган анъанавий криптографик алгоритмлар кўпинча ҳисоблаш ресурсларининг чекланганлиги (масалан, сенсорли тармоқларда) ёки янги турдаги киберҳужумларнинг ривожланиши сабабли етарли самара бермаяпти. Шу билан бирга, квант ҳисоблаш тизимларининг ривожланиши яқин келажакда классик криптоалгоритмларнинг бардошлилигига жиддий хавф туғдириши прогноз қилинмоқда. Бу эса мавжуд алгоритмларни криптотаҳлил қилиш ва уларнинг чизиқсизлик хусусиятларини мунтазам баҳолаб боришнинг долзарблигини белгилайди.

Муаммонинг қўйилиши. Криптология соҳасида криптография (шифрлаш усулларини яратиш) ва криптоанализ (уларни таҳлил

қилиш ва заифликларини топиш) бир-бирини тўлдирувчи икки жабҳа сифатида параллел ривожланиб келмоқда. Бироқ, амалиётда криптографик алгоритмларни таҳлил қилиш жараёни ҳар бир алгоритм учун индивидуал ёндашувни, мураккаб математик аппаратни ва юқори малакали мутахассислар меҳнатини талаб этади. Ҳозирги кунда жаҳон миқёсида турли шифрлаш алгоритмларини (AES, PRESENT, ASCON, маҳаллий стандартлар ва бошқалар) ягона мезонлар асосида комплекс таҳлил қилувчи универсал автоматлаштирилган тизимларнинг тақчиллиги сезилмоқда.

Мавжуд дастурий воситаларнинг кўпчилиги ёпиқ тизимлар бўлиб, улар янги яратилаётган енгил вазнли (lightweight) алгоритмларни ёки миллий криптографик стандартларни мослашувчан тарзда текшириш имкониятини бермайди. Қўлда (manual) бажариладиган криптотаҳлил жараёнлари эса инсон омилига боғлиқ бўлиб, вақт ва хатоликлар эҳтимоли жиҳатидан самарасиздир. Бу эса ўз навбатида, S-блокларнинг (S-boxes) криптографик кўрсаткичларини автоматлаштирилган ҳолда текширувчи, тизимли ва тезкор дастурий мажмуани ишлаб чиқиш зарурiятини юзага келтиради.

Тадқиқотнинг мақсади ва вазифалари. Ушбу монографиянинг асосий мақсади — симметрик блокли шифрлаш алгоритмларининг бардошлилигини белгиловчи асосий ночизиқли элемент — S-блокларни комплекс криптографик баҳолашнинг назарий асосларини ва уни амалга оширувчи автоматлаштирилган дастурий воситани ишлаб чиқишдан иборат.

Тадқиқот давомида қуйидаги муҳим вазифаларга эътибор

қаратилади:

Симметрик блокли шифрлаш алгоритмларида S-блокларга қўйиладиган замонавий криптографик талабларни таҳлил қилиш ва тизимлаштириш.

S-блокларнинг чизиқсизлик даражаси (Nonlinearity), алгебраик нормал шакли (ANF), қатъий лавина эффекти (SAC), бибитли мувофиқлик ва дифференциал бир хиллик каби кўрсаткичларини ҳисоблаш алгоритмларини оптималлаштириш.

Турли ўлчамдаги (4x4, 8x8 ва ҳ.к.) S-жадвалларни таҳлил қила оладиган, фойдаланувчи учун қулай интерфейсга эга бўлган универсал дастурий мажмуа (Delphi ёки бошқа муҳитларда) архитектурасини лойиҳалаш.

Ишлаб чиқилган восита ёрдамида мавжуд халқаро (AES, ASCON, PRESENT) ва миллий криптоалгоритмларнинг хавфсизлик кўрсаткичларини қиёсий таҳлил қилиш.

Тадқиқотнинг объекти ва предмети. Тадқиқот объекти сифатида ахборотни ҳимоялашнинг симметрик блокли шифрлаш алгоритмлари ва уларнинг таркибий қисми бўлган S-блоклар олинган. Тадқиқот предмети эса ушбу S-блокларнинг криптографик бардошлилик кўрсаткичларини баҳолаш усуллари ва уларни автоматлаштириш технологияларидан иборат.

Илмий ва амалий аҳамияти. Монографияда келтирилган натижалар криптографик тизимларни лойиҳалаш билан шуғулланувчи ташкилотлар ва мутахассислар учун муҳим методик манба бўлиб хизмат қилади. Яратилган автоматлаштирилган дастурий восита янги алгоритмларни ишлаб чиқишда энг мақбул ва бардошли S-блокларни

танлаб олиш имконини беради. Бу эса ахборот хавфсизлиги соҳасида маҳаллий дастурий маҳсулотлар улушини оширишга, киберҳужумларга қарши барқарор тизимларни яратишга ва соҳа мутахассисларининг тайёргарлик даражасини юксалтиришга хизмат қилади.

I боб. КРИПТОГРАФИК АЛГОРИТМЛАРНИ КРИПТОАНАЛИЗ ҚИЛИШ УСУЛЛАРИНИНГ ТАҲЛИЛИ

1.1. Классик алгоритмларни криптотаҳлиллаш усулларининг тадқиқи

Охирги йигирма йил ичида криптотаҳлил фаол ривожланаётган тадқиқот соҳаларидан бирига айланди. Бу вақтда криптотаҳлилчиларда қизиқиш уйғотадиган математик усулларнинг бутун бир арсенали яратилди. Бундан ташқари, ҳисоблаш техникаси самарадорлиги ошиши натижасида аввал мавжуд бўлмаган ҳужум турларининг пайдо бўлишига олиб келди. Қуйидаги 1.1-жадвалда криптотаҳлил усулларининг пайдо бўлиши вақт бўйича ва турли хил криптотизимларни бузишда қўлланилиши бўйича тизимлаштирилган маълумот келтирилган.[1]

1.1-жадвал

Криптотаҳлил усуллари

Хэш-функция		5, 8	10
Носимметрик шифр		1, 2, 3, 4	9,10
Симметрик шифр	1, 2	3, 6, 7	9,10
	Кеча	Бугун	Келажакда

Бу ерда:

1 - Калитларни тўлиқ танлаш усули.

2 - Частотавий таҳлил усули.

3 - Калит генератори таҳлили.

4 – Поллард усули.

5 - «Ўртада учрашиш» усули.

6 - Дифференциал таҳлил усули.

7 - Чизиқли таҳлил усули.

8 - Коллизия усули.

9 - Қўшимча каналлар бўйича таҳлил усули

10. Квант таҳлили

Ҳар қандай криптотизимнинг бардошлилиги криптоалгоритмга ва калитнинг хоссаларига эга бўлиши билан бир қаторда ишончли пухта протоколга ҳам эга бўлиши шарт. Пухта математик асосга эга бўлиб, мукаммал баённомага эга бўлмаган криптотизим заиф ва бардошсиз бўлиши мумкин.

Криптотизимларни криптотаҳлиллашнинг универсал усуллари қаторига ҳозирги кунда қўлланиб келинаётган ва самарали натижа берадиган тўлиқ танлаш, частотавий таҳлил, ўртада учрашиш, Поллард, калит бўйича ҳужум ва хэш-функция коллизияси усулларини ҳамда қўшимча каналлардан фойдаланишга асосланган криптотаҳлил усулларини киритиш мумкин.

Тўлиқ танлаш усули, яъни калитларнинг барча мумкин бўлган вариантларини танлаш усули, криптотаҳлилчининг носимметрик криптотизим алгоритмини ва ошкора калитни билган ҳолда барча мумкин бўлган калитларни танлаш ва синаб кўришга асосланади. Симметрик криптотизимларда ҳам шифрматн ва очиқ матн асосида тўлиқ танлаш усули қўлланилади. Криптотаҳлилчилар кўпинча компьютер ёрдамида калитларни тўлиқ танлаш усулидан фойдаланиб шифрларни ошкор этадилар. Криптотаҳлил жараёнида миллиард

калитларни секундига минглаб калит тезликда танлашга тўғри келади.[2]

Фараз қилинсин, бузғунчи учун бир ёки бир неча (x, y) жуфтлик маълум бўлсин. Осонлик учун ҳар қандай жуфтлик (x, y) учун $Ek(x) = y$ муносабатни қаноатлантирувчи ягона k калит мавжуд бўлсин. Мумкин бўлган калитлар тўпламини тартибга солинади ва K даги калитларни кетма-кет равишда $E_k(x) = y$ тенглик бажарилишига текшириб чиқилади. Агар $k \in K$ калитнинг бир вариантини текшириш бир амал ёрдамида ҳисобланса, унда калитларни тўлиқ танлаш учун $|K|$ амал талаб этилади. Бунда $|K|$ - тўпламдаги элементлар сони. Шифрлаш схемасида калит тасодифий ва тенг эҳтимоллик билан K тўпламдан танланган бўлсин. Бунда калит $1/|K|$ эҳтимоллик билан топилади ва тўлиқ танлаш усулининг иш ҳажми *1* га тенг бўлади.

Мисол учун шахсий калит узунлиги *100* бит бўлса, унда барча шахсий калитлар сони 2^{100} га тенг, яъни калитлар тўплами қуввати $|K| = 2^{100}$. Шахсий калит узунлиги *56* бит бўлганда, барча мумкин бўлган шахсий калитлар сони $|K| = 2^{56} \approx 0.5 * 10^{17}$ га тенг. Бунда, агар ҳисоблаш қурилмаси ҳар битта махфий калитга мос ошкора калитни ҳисоблаш ва уни ҳеч қийинчиликсиз таққослаш учун 10^{-6} секунд вақт сарфласа, *24* соатда барча калитларни синаб чиқиш учун $5.787*10^5$ та ЭҲМ керак бўлади.

Шунинг учун ҳам шахсий ва шифрлашда фойдаланиладиган калитни топишни мураккаблаштириш мақсадида шахсий калитлар узунлиги *127-159* битдан катта бўлган узунликда генерацияланади.

*Калит бўйича ҳужум усули***.**Криптотаҳлилчининг махфий калитни топишга қаратилган хатти-ҳаракатлари криптоҳужум деб

аталади.

Криптоҳужумдан мақсад калитни билмаган ҳолда шифрматнни очишдир. Криптотизимга ҳужум қилиш учун криптотаҳлилчи зарурий криптотаҳлил воситаларига эга бўлиши керак. Бу воситалар криптоҳужум қўлланиладиган шифрлаш алгоритмининг акслантиришлари хусусиятларини ҳисобга олиб, шифрматнни шифрлаш алгоритми калитини билмаган ҳолатда шифрматнни очиш мақсадида математик моделлаштириш усулларини қўллаш асосида яратилади.

Криптотизимнинг ишончсизлиги сабабларидан бири тизимда кучсиз калитлардан фойдаланиш ҳисобланади, чунки кучсиз калитлар етарли даражада ҳимоялаш даражасини таъминлай олмайди. Шу сабабли калитларни ҳосил қилиш жараёнида уларни яроқсизга чиқариш учун барча кучсиз калитлар аввалдан маълум бўлиши лозим. Тасодифий сон генераторлари криптографик тизимларнинг бардошлилиги учун яна бир хавф манбаидир. Агар калитларни генерациялашда кучсиз криптографик алгоритмлардан фойдаланилса, фойдаланилган шифрдан қатъий назар бутун тизим бардошсиз ҳисобланади.[6]

Симметрик криптотизимларда фойдаланиш учун мўлжалланган сифатли калит тасодифий иккилик тўпламини ифодалайди. Агар n разрядли калит талаб этилса, калитни генерациялаш жараёнида мумкин бўлган 2^n вариантлардан бир хил эҳтимоллик билан танлаб олиш керак.

Носимметрик криптотизимларда фойдаланиш учун мўлжалланган сифатли калитларни генерациялаш эса анча қийин

жараён бўлиб, юқорида айтилганидек бу тизимда фойдаланиладиган калитлар муайян математик хоссаларга эга бўлиши лозим. Масалан, RSA тизимида шифрлаш модули иккита катта туб сонларнинг кўпайтмаси кўринишида бўлади.

Псевдотасодифий генераторлар ёрдамида бардошли криптотизимларни яратиш мумкин. Яхши тасодифий сон генераторлари ишлаб чиқишда мураккаб бўлиб, уларнинг ишончлилиги аппарат ва дастурий таъминотнинг афзаллигига боғлиқ бўлади. Шу сабабдан турли криптографик қарашлар асосида самарали псевдотасодифий генераторлар яратиш бўйича тадқиқотлар амалга оширилмоқда.

Частотавий таҳлил усули. Частотавий, яъни статистик характеристикалар усулида симметрик ёки носимметрик криптотизим криптотаҳлилчиси шифрматндаги белгилар, ҳарфлар, сўзларнинг такрорланишлари сонини (частоталарини) ҳисоблаб, очиқ матн қайси тилда ёзилганини аниқлайди. Сўнгра эса, шифрматн шифр белгилари параметрларини очиқ матн қайси тилда ёзилган бўлса, шу тилнинг параметрлари билан солиштиради. Масалан, инглиз тилида E ҳарфи частотаси юқори, шифрматнда L ҳарфи частотаси юқори. Шифрматндаги L ҳарфини E ҳарфи билан алмаштирилади, яъни шифрматн ва очиқ матн ёзилган тил частоталарини камайиш тартибида ёзиб, тартиби тўғри келган белгилар ўзаро алмаштирилади. Кейин шифрматн биграмма, триграмма ва k-граммаларининг такрорланишлар сонини топиб, очиқ матн ёзилган тил биграмма, триграмма ва k-граммалари билан мос ҳолда алмаштиради. Биграмма, триграмма, k-грамма деганда, матнда иккита, учта ва k-та белгининг

кетма-кет келиши тушунилади. Масалан, инглиз тилида th, in, is, er, he, en, биграммалари, рус тилида ст, но, ен, то, на биграммалари, сто, ено, нов, тов, ова триграммалари кўп учрайди. Қуйидаги 1.2-жадвалда рус тили ҳарфларининг пайдо бўлишининг нисбий частотаси келтирилган.[6,12]

1.2-жадвал

Рус тили ҳарфларининг пайдо бўлишининг нисбий частотаси

Ҳарф	**Частота**	**Ҳарф**	**Частота**	**Ҳарф**	**Частота**	**Ҳарф**	**Частота**
о	0.09	О	0.038	о	0.016	О	0.007
е,ё	0.072	Л	0.035	ы	0.016	Ш	0.006
а	0.062	К	0.028	б	0.014	Ю	0.006
и	0.062	М	0.026	ь, ъ	0.014	Ц	0.004
н	0.053	Д	0.025	г	0.013	Щ	0.003
т	0.053	П	0.023	ч	0.012	Э	0.003
с	0.045	У	0.021	й	0.01	Ф	0.002
р	0.04	Я	0.018	х	0.009		

Юқорида айтиб ўтилган принциплар ҳозирги кунда кенг тарқалган паролларни танлаш бўйича дастурларда қўлланилади. Паролларни танлаш бўйича дастур аввало эҳтимоллиги катта бўлган паролларни танлайди. эҳтимоллиги кичик бўлган паролларни кейинга олиб қўяди. Бунда паролларни танлаш жараёни ўн ва юз мартталаб камаяди. Қуйидаги 1.3-жадвалда паролларни танлашда олинган қатор натижалар келтирилган.

1.3-жадвал

Паролларни танлаш натижалари

Танлаш мураккаблиги	**Танлаш вақти**	**Процессор тури**
$2{,}08 \cdot 10^{11}$	15 минут	486DX/4-100
$5{,}68 \cdot 10^{10}$	8 соат	Pentium-120

Поллард усули. Поллард усули график шаклда "ўртада учрашиш" усулига бироз ўхшашдир. Унда "тасодифий акслантириш графида учрашиш" масаласи ечилади. Бу ерда ҳам иккита графнинг бошланғич тугунларидан чиқиб токи илдиз тугунидан ўтувчи цикл ҳосил бўлгунча қарама-қарши йўналишда ҳаракат давом этади. Учрашиш мураккаблиги $0{,}5\varphi(p/8)\#\grave{I}$, якуний мураккаблик $6{,}5\varphi(p/8)\#\grave{I}$.

Поллард усули циклик группада дискрет логарифм масаласини ечиш учун қисман эквивалент калитларни топишда қўлланилади. Булар бир хил хэш-функция берувчи икки аргументни топишда ҳам асқотади.

Дискрет логарифмлаш масаласига тадбиқан бу усул аввалги "ўртада учрашиш" усулига нисбатан катта хотирадан воз кечиш имконини яратади. МБни сортлаш зарурати ҳам йўқолади. Шу туфайли вақт бўйича мураккаблик $0(log\#M)$ марта кам бўлиб, мураккаблик $O(\varphi\#M)$ қадам, хотира ҳажми $0(1)$ блокдан иборат.

«Ўртада учрашиш» ҳужум усули. Агар криптоалгоритмнинг махфий калитлар тўплами композиция амалига нисбатан берк бўлса, яъни ҳар қандай икки калит z_i ва z_j учун шундай калит z_k топилсинки,

ҳар қандай матни кетма-кет z_i ва z_j калитларида шифрлаш натижаси шу матнни z_k билан шифрланган матнга айнан бўлсин, яъни

$$F(z_j, F(z_i, x)) = F(z_k, x).$$

Унда бу хоссадан фойдаланиб, шифрлаш калитини топиш мумкин, яъни z_k ни топиш учун эквивалент жуфтлик $< z_i, z_j >$ ни топиш кифоя. Бу усул "туғилган кунлар парадокси"га асосланади. Маълумки, туғилган кунлар текис тақсимланган деб ҳисобланса, 24 кишилик гуруҳда $\mathrm{p} = 0{,}5$ эҳтимоллик билан икки кишининг туғилган куни бир хил чиқади.

Умумий ҳолда бу парадокс қуйидагича ифодаланади: агар $\mathrm{a} \in n$ предметлар n та предмет орасидан қайтарилиш билан танланса, икки предметнинг бир хил бўлиш эҳтимоли

$$\mathrm{p} = 1 - \mathrm{e}^{-\mathrm{a}^2/2}.$$

Фараз қилинсинки, очиқ матн x ва у нинг шифрограммаси у маълум. x учун тасодифий тарзда калитлар тўплами z_l ва шифрограммалар

$w = F(z_l, x)$ тўпламини сақловчи маълумотлар базаси (МБ) тузамиз ва шифрограммаларни w бўйича тартибга соламиз. МБ ҳажмини $0((p\#\{z\})$ га тенг қилиб оламиз.

Сўнгра тасодифан z_{l1}калитни олиб,у шифрматнни очамиз ва натижа $v = F(z_{l1}, \mathrm{y})$ ни МБ билан таққослаймиз. Агар v бирор w билан тенг чиқса, калит z_{l1}изланган калит z га эквивалент.[12]

Вақт бўйича усул мураккаблиги

$$\mathrm{O}(\varphi\#\{\mathrm{z}\}\log\#\{\mathrm{z}\}).$$

Кўпайтувчи $log\#\{z\}$ саралаш мураккаблигини ҳисобга олади.

Зарур хотира $O((\text{р}\,\#\{z\}log\#\{z\})$ бит ёки $O((\text{р}\,\#\{z\})$ блокдан иборат. Блок узунлиги ва калит узунлиги чекланган доимийга фарқ қилади деб фараз қилинади.

Бу усул калитлар тўплами яримгруппа бўлган қисм тўпламни ўз ичига олган бўлса ҳам қўлланилиши мумкин. Бу усулнинг бошқа қўлланилишини тўплам яримгруппа бўлмаган ҳол учун хэш-функциялар мисолида намойиш этиш мумкин.

Масалан, ЭРИни сохталаштириш учун битта хэш-образга эга икки матн топиш лозим. Ундан сўнг имзоланган хабарни бошқа ўша хэш-образга эга бўлган хабар билан алмаштириб қўйиш мумкин. Бундай икки хабарни топишни "ўзаро учрашиш" усулида амалга оширилса, излаш мураккаблиги

$$O((p\ \#\{z\})$$ бўлади.

Бунда $\#\{z\}$ мумкин бўлган хэш-образлар сони. Америкалик математик Д. Шенкс томонидан таклиф этилтан бу алгоритм эҳтимоллик алгоритмидир. *Хэш-функция коллизияси усули.*
Криптографияда хэш-функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

- маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;

- маълумотнинг манбасини аутентификация қилиш учун.

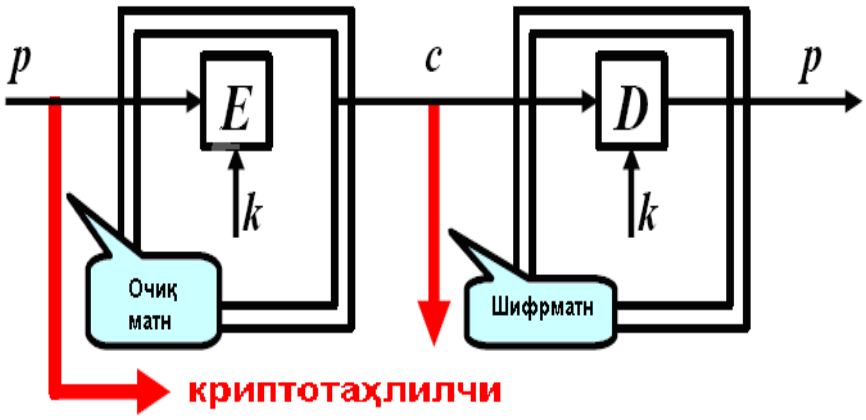
Маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун ҳар бир маълумотнинг хэш-қиймати ҳисобланади ва бу қиймат маълумот билан бирга сақланади ёки узатилади. Маълумотни қабул қилган фойдаланувчи маълумотнинг хэш-қийматини ҳисоблайди ва мавжуд бўлган назорат қиймати билан солиштиради.

Агар таққослашда бу қийматлар мос келмаса, маълумот ўзгарганлигини билдиради.

Хэш-функцияларга қилинадиган асосий ҳужум бу коллизияни ҳосил қилишдир. Қўлга тушган x ва $y \neq$ x матнлар учун H(x) $\neq H(y)$ бўлиши - коллизияга бардошлилик хоссасидир.

“Туғилган кун парадокси”га асосланган криптоҳужум хэш-функцияларда коллизияларни топиш учун ишлатиладиган асосий криптоҳужумлардан биридир. Бу криптоҳужумга асосан хэш-қиймат берилганда унга мос бўлган маълумотни танлашнинг мураккаблиги $O(2^n)$ катталик билан, маълумот ва унинг хэш-қиймати берилганда, хэш-қиймати шунга тенг бўладиган бошқа маълумотни танлашнинг мураккаблиги $O(2^{n/2})$ катталик билан баҳоланади. H(x) $= H(y)$ кўринишдаги иккита маълумотни “ўртада учрашиш” ёки Поллард усулидан фойдаланиб топиш мумкин.

Қўшимча каналлардан фойдаланишга асосланган криптотаҳлил усули. Бошқа томонлар ва қўшимча каналлар орқали ҳужум – бу криптографик ҳужум тури бўлиб бошқа томонлар ва қўшимча каналлардан олинган ахборотлардан фойдалан ишга асосланган. Қўшимча каналлардан олинган ахборот деганда шифрлаш қурилмасидан олиниши мумкин бўлган ахборот тушунилади, бунда у очиқ ёки шифрматн ҳисобланмайди (1.1-расм).



1.1-расм. Қўшимча каналлар орқали ҳужум

Қўшимча каналлар орқали ҳужум қуйидаги уч тур буйича таснифланади.

- ҳисоблаш жараёнини назорат қилиш бўйича: фаол ва суст;

- модулдан фойдаланиш усули бўйича: агрессив, ярим агрессив ва ноагрессив;

- таҳлил жараёнида қўлланиладиган услуб бўйича: оддий ва турлича.

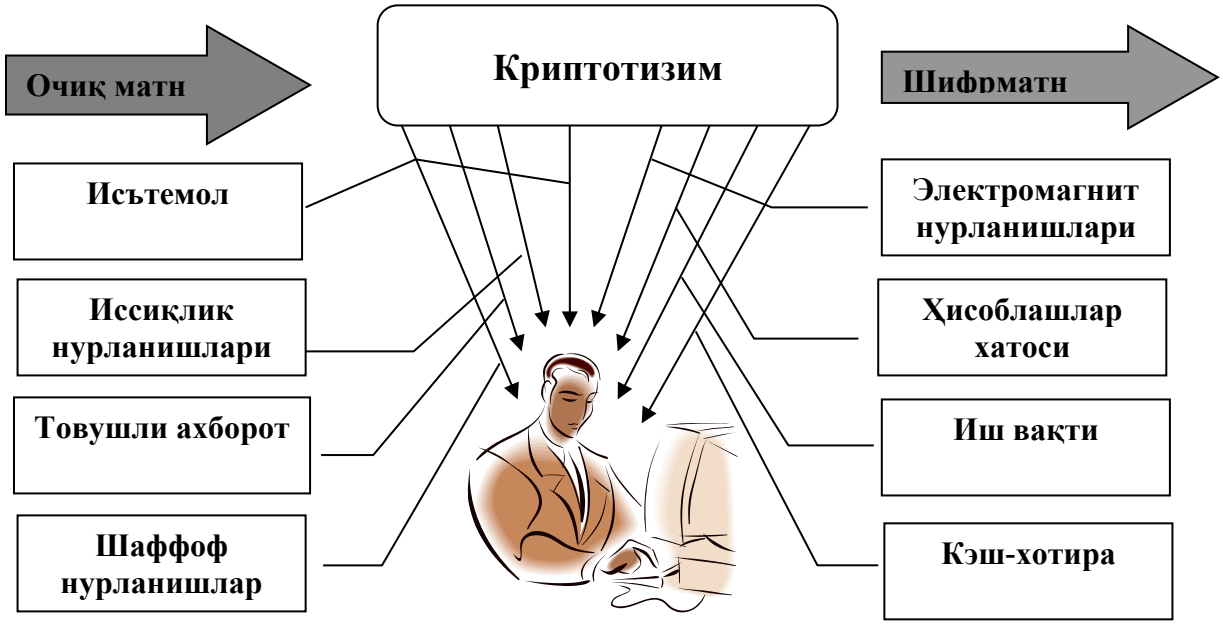
Қўшимча каналлар орқали қилинадиган ҳужумларда криптографик алгоритм ва протоколларни реализация қилишда олинган ахборотлардан фойдаланилади. Бу маълумотлар вақт ўлчови бўйича, қувват ёки электромагнит нурланиш сарфи бўйича бўлиши мумкин. Қўшимча каналлардан олинадиган ахборотларнинг бошқа шакли сифатида дастурий ёки аппарат хатоларини ҳисоблаш натижалари бўлиши мумкин.

Бундан криптографик алгоритмларни дастурий ёки аппаратли реализациясини аниқ амалга ошириш хавфсизлик учун жуда муҳимлиги келиб чиқади. Кичкина бир хатолик хавфсизликда катта фарқни келтириб чиқаради. Ҳозирги кунда ўндан ошиқ қўшимча

каналлар фарқланади . Қуйидаги 2-расмда баъзи қўшимча каналлар келтирилган.

Ҳужумлар фойдаланиладиган қўшимча каналлар кўринишига қараб ажратилади. Қуйида қўшимча каналлар орқали қилинадиган машҳур ҳужумларни санаб ўтамиз.[14]

1. Вақт бўйича ҳужум.
2. Қувват бўйича оддий ҳужум.
3. Қувватлар фарқи бўйича ҳужум.
4. Ҳисоблашлар хатоси бўйича ҳужум.
5. Электромагнит нурланишлар бўйича ҳужум.
6. Шаффоф нурланишлар бўйича ҳужум.
7. Акустик ҳужум.
8. Кэшга ҳужум.



1.2-расм. Қўшимча каналлар

Қўшимча каналлар орқали қилинган *вақт бўйича ҳужум* даставвал фуқаролар уруши даврида пайдо бўлган. Криптографик

алгоритмларни амалга оширишдаги ҳисоблашлар турли вақт оралиқларида бажарилади. Бу вақт ичида махфий параметрлар ҳақида баъзи ахборотларга эга бўлиш мумкин ва агар ҳужумни аниқ амалга ошириш бўйича етарли билимга эга бўлса, унда статистик таҳлил мазкур махфий параметрларни тўлиқ тиклаши мумкин бўлади. Вақт бўйича ҳужум шифрлаш жараёнини бажариш учун зарур бўлган шифрлаш модулини топиш вақтини аниқ ўлчашга асосланган. Бу ахборот махфий калитни очиш имконини беради.

Қувват бўйича ҳужумдан, асосан, криптотизимлар аппарат кўринишда амалга оширилганда, фойдаланилади. Қувват бўйича ҳужум айниқса махфий калит сақланадиган смарт-карта ва бошқа тизимларга ҳужумда муваффақиятли бўлади. Қувватлар фарқи бўйича ҳужум эса истеъмол қилинадиган қувватни таҳлил этиш натижасида амалга оширилади. Смарт-карталарга қувват бўйича оддий ҳужум одатда бир неча секундни, қувватлар фарқи бўйича ҳужум эса бир неча соатни талаб этади. Қувватлар фарқи бўйича ҳужум энг кам сарфни талаб этади.

Ҳисоблашлар хатоси бўйича ҳужум аппарат таъминотидаги тасодифий хатоликларга қаратилган бўлиб, унинг хавфсизлигига жиддий таъсир кўрсатади. Бу хатоликлар ёки хато чиқиш маълумотларининг муҳим қўшимча каналга айланишини, ҳатто баъзида криптотаҳлил учун шифрнинг заифлигини сезиларли ошириб юборади.

Ҳисоблаш амалларини компьютерларда амалга ошириш электромагнит нурланишларни юзага келтиради. Бу нурланишларни ўлчаш ва таҳлиллаш натижасида криптотаҳлилчи бажарилаётган

ҳисоблашлар ва фойдаланилаётган маълумотлар тўғрисида аҳамиятга молик ахборотга эга бўлади.

Электромагнит нурланишлар бўйича ҳужум билан бирга шаффоф нурланишлар бўйича ҳужумдан ҳам фойдаланилади. Бунда компьютер мониторидан чиққан нурланишнинг девордаги акси чиқиш сигналларини тиклашга ёрдам бериши мумкин. Бу ҳужумнинг афзаллиги шундаки, бунда қурилмадан фойдаланиш талаб этилмайди.

Ҳозирги вақтда қўшимча каналларни тадқиқ этиш асосан энергия истеъмолини таҳлил этиш бўйича ҳужумга йўналтирилган бўлса ҳам, *акустик ҳужум* хавфи мавжуддир. Процессорнинг товуши билан унда бажариладиган ҳисоблашлар орасида боғлиқлиқ борлигини криптотаҳлилчи Шамир исботлаб берган.

Агар процессор кэш-хотирада сақланмаётган маълумотлардан фойдаланишни амалга оширса, зарурий маълумотлар кэш-хотирадаги асосий хотирадан юкланмагунча ҳисоблашларда қандайдир тўхтаб қолиш содир бўлади. Бундай тўхтаб қолиш бузғунчи учун кэш-хотирани тўлиш частотасини аниқлаш имконини беради. Худди шу ердан қўшимча каналга ахборот сизиб чиқиши юзага келади.

Юқорида келтирилган криптотаҳлил усллари классик шифрлаш алгоритмларига қаратилган бўлиб, асосан шу турдаги шифрлаш алгоритмларига ҳужум уюштириш ёки алгоритмлар бардошлилиги ҳисоблаш учун хизмат қилаи. Бироқ бугунги кунда ҳисоблаш техникаси имкониятларининг юқорилиги боис, амалда классик шифрлаш алгоритмлари қўлланилмайди. Шундан келиб чиқиб классик алгоритмларни криптотаҳлиллаш осон ҳисобланади. [43]

Бугунги кунда шифрлаш тезлигининг юқорилиги ва криптобардошлилиги билан симметрик алгоритмлар алоҳида аҳамият касб этади. Бироқ барча симетрик шифрлаш алгоритмларининг барчасини бардошли деб бўлмайди. Уларнинг бардошлилигини исботлаш учун криптотаҳлил усулларидан фойдаланилади. Шундан келиб чиқиб диссертация ишининг навбатдаг бўлими симметрик шифрлаш алгоритмларини криптотаҳллаш усуларини тадқиқ қилишга бағишланади.

1.2. Симметрик шифрлаш алгоритмларини криптотаҳлиллаш усулларининг тадқиқи

Махфий ахборотни ошкор қилишга заруриятлар, криптографик алгоритмларнинг бардошлилигини текширишдаги изланишлар натижасида криптоанализ йуналиши вужудга келди ва ривожланмоқда. Шу жумладан симметрик блокли шифрлаш алгоритмларига қаратилган бир нечта криптоанализлаш усуллари яратилди. Қуйидаги усулларни келтириш мумкин:

1. Чизиқли криптоанализ усули;
2. Дифференциал криптоанализ усули;
3. Чизиқли-дифференциал криптоанализ усули;
4. Слайдли ҳужум криптоанализ усули;
5. Алгебраик криптоанализ усули;
6. Интеграл криптоанализ усули ;

Чизиқли криптоанализ усули. Замонавий чизиқли криптоанализ усули Япониялик криптограф M.Matsui томонидан 1993 йилда DES шифрлаш алгоритмига қарши ҳужум тури сифатида ишлаб чиқилган.[43,68]

Ушбу криптоанализ усулининг моҳияти танлаб олинган очиқ матн M ва мавжуд шифрматн C битларини XOR амали ёрдамида қўшиш ва натижада калит битларини аниқлашдан иборат:

$$M[i_1, i_2, \dots . i_n) \oplus C[j_1, j_2, \dots . j_n] = K[k_1, k_2, \dots . k_n],$$

бу ерда $M[i_1, i_2, \dots . i_n) = M[i_1) \oplus M[i_2) \oplus \dots . M[i_n)$

$$\mathrm{C}[i_1, i_2, \dots . i_n) = \mathrm{C}[i_1) \oplus \mathrm{C}[i_2) \oplus \dots . \mathrm{C}[i_n)$$

$$K[i_1, i_2, \dots . i_n) = K[i_1) \oplus K[i_2) \oplus \dots . K[i_n)$$

Натижада юқоридаги тенгликдан энг яқин чизиқли аппроксимацияни аниқлаш, яъни таҳлил қилинаётган алгоритм акслантиришлари хоссаларидан келиб чиқиб, энг самарали чизиқли боғланишни танлашдан иборат. Танланган аппроксимация тенгламаларида тенгликнинг чап томонининг қиймати 0 ёки 1 эканлигини аниқлаш учун етарлича кўп миқдордаги очиқ матн ва шифр матн жуфтликлари устида статистик таҳлил олиб бориш керак бўлади. Натижада, фақат калит битлари иштирок этган тенгламалар системасига эга бўлинади. Ушбу тенгламалар системасини ечиш орқали калит битларини аниқлаш мумкин бўлади.

Умуман симметрик блокли шифрлаш алгоритмларида чизиқсиз акслантиришлар S-блоклар бўлиб ҳисобланади. Демак S-блокларини криптоанализ қилиш асосида алгоритмнинг криптобардошлилиги хусусида хулоса билдириш мумкин. S–блокларни чизиқли криптоанализ қилиш учун чизиқли аппроксимация тенгламаларини тузиш керак. Бунда “корреляцион матрица” жадвалидан фойдаланиш самарали усул ҳисобланиб, айнан ушбу жадвал чизиқли криптоанализнинг асосий характеристикаси ҳисобланади.

Корреляцион матрицани тузиш қуйидагича амалга оширилади. Масалан, шифрлаш алгоритмида $Y = \varphi(X): GF(2^n) \to GF(2^m)$ чизиқсиз акслантириш бажарилган бўлсин. Яъни, X$[x_1, x_2, \dots . x_n)$ – акслантиришга кирувчи битларни, Y$[y_1, y_2, \dots . y_n)$–акслантиришдан чиқувчи битларни ифодалайди.

Таъриф. $Y = \varphi(X)$ - акслантиришга нисбатан корреляцион матрица деб, ҳар бир (*i*,*j*) - элементи қуйидаги тенглик билан аниқланувчи *C* – жадвалга айтилади:

$$C(\mathrm{i},\mathrm{j}) = \#\{X < X, i >= Y < Y, j >\} \text{ бу ерда}$$

$$i \in 2^n, j \in 2^m,$$

$$< X, i > [x_1 i_1 \oplus x_2 i_2 \oplus, \dots . x_n i_n),$$

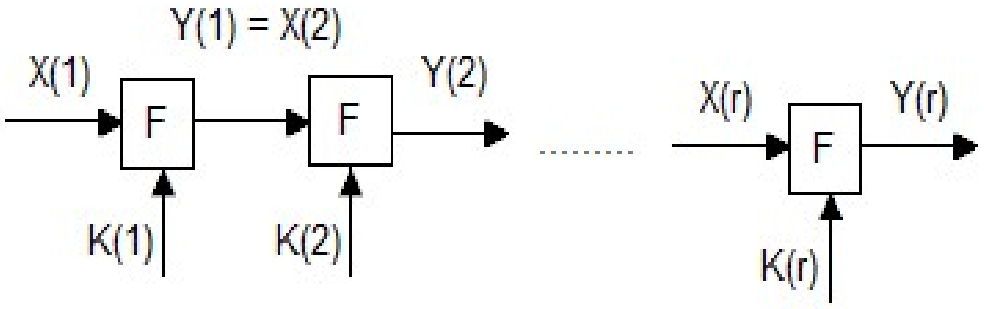
$$< Y, i > [y_1 i_1 \oplus y_2 i_2 \oplus, \dots . y_n i_n)$$

Таърифдан корреляцион матрица акслантиришга кирувчи ва чиқувчи битлар хар ҳил позицияларининг ўзаро боғланишларини, яъни кирувчи *i*–битларни XOR амали ёрдамида йиғиндисининг чиқувчи *j*–битларни XOR амали ёрдамида йиғиндисига неча марта тенг бўлишини ифодалайди.

Дифференциал криптоанализ (ДК) ҳисобланади. ДК усули Исроил криптографлари E.Biham ва A.Shamir томонидан 1990 йилда DES алгоритмига қарши ҳужум тури сифатида ишлаб чиқилган. ДК усулида шифрлаш алгоритми, унга мос танлаб олинган очиқ матн ва шифр матн маълум деб олинади. Мазкур криптоанализ усули стандарт 16-раундли DES алгоритмини амалий жиҳатдан тўлиқ очиш имкониятини бермаса ҳам (247 та матн керак бўлади), қисқартирилган

раундли масалан, 8-раундли, 6-раундли DES алгоритмини муваффақиятли очиш имконини беради.[14,68]

ДК усулининг моҳияти бирор алгоритмга кирувчи X, X' ва унинг айирмаси ΔX, чиқувчи Y, Y' ҳамда унинг айирмаси ΔY қийматлардан фойдаланиб калитни топишдан иборатдир. Мазкур усулни амалиётда қўллаш мураккаблиги шундан иборатки, етарлича кўп миқдордаги очиқ матн ва шифр матн жуфтликлари устида таҳлил олиб бориш керак бўлади.



1.3-расм. Блокли шифрлаш схемаси

ДК усулини ифодалаш учун блок узунлиги N га тенг бўлган шифратор қуйидаги –расмда кўрсатилган схемадагидек бўлсин. Бу ерда $K = (K(1), K(2), \dots, K(r))$ калитлар K_0 калитдан бирор қонуният асосида ясалган ёки хар бир роунд учун алоҳида танланган калитлар, X(1) ва X'(1) очиқ матн жуфтликлари.

Қуйидаги фарқлар кўриб чиқилсин:

$$\Delta X(1) = X(1) - X'(1);$$

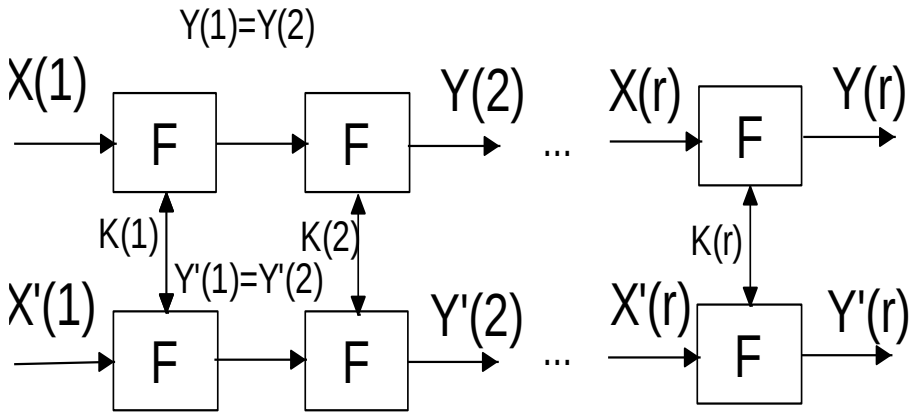
$$\Delta Y(i) = Y(i) - Y'(i).$$

Дифференциал криптоанализнинг вазифаси, $X(1), K(1), K(2), \dots, K(r-1)$ маълумотларни $1/(2^N)$ эҳтимоллик

билан танлаш орқали $\Delta Y(r-1)$ шифрматн фарқига мос $\Delta X(1)$ очиқ матнлар фарқини тонишдан иборат.

(α, β) жуфтлик $(\Delta X(1), \Delta Y(i))$ векторларнинг I-циклдаги дифференциали дейилади.

Шунда дифференциал криптотахлилни қуйидаги 1.4–расмда кўрсатилган моделдек тасвирлаш мумкин.



1.4-расм. Дифференциал криптоанализ модели

Шифрнинг охирги роунд калитини қўйидаги алгоритмлар кетма-кетлиги асосида топилади:

1. $P(\Delta X(1) = \alpha, \Delta Y(r-1) = \beta$ катта эҳтимолликлар учун, $(r-1)$ циклнинг дифференциали (α, β) танланади;

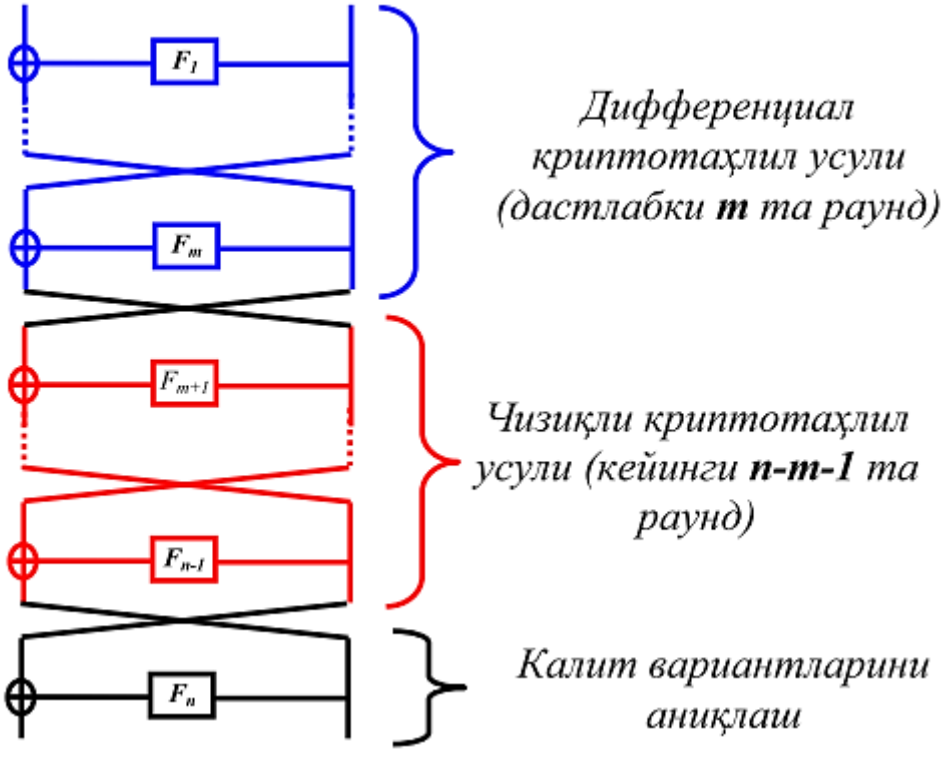
2. X(1) тасодифий танланади. Маълум $Y(r), Y'(r)$ ва $\Delta X(1) = \alpha$ тенглик асосида $X'(1)$ танланади;

3. Тахмин қилинган ΔY(r-1) $= \beta$ ва маълум $Y(r), Y'(r)$ лардан фойдаланиб К(r) топилади;

4. Иккинчи ва учунчи қадамлар калитлар кесишмаси ягона элементни қабул қилмагунча давом эттирилади.

Чизиқли-дифференциал криптоанализ усули 1994 йилда Мартин Хеллман ва Сьюзен Лангфорд томонидан DES шифрлаш алгоритмига қарши ҳужум тури сифатида ишлаб чиқилган. Ушбу усул танланган

очиқ матнга асосланган бўлиб, ғоя муаллифлари томонидан Чизиқли-дифференциал криптоанализ (ЧДК) усулини қўллаб, 512 та очиқ матн ёрдамида DES шифрлаш алгоритмида фойдаланилган махфий калитнинг 10 битини 80% эҳтимоллик билан аниқлашга эришилган. Очиқ матн сонини 768 тага ошириш орқали бу эҳтимоллик қийматини 95% гача етказиш мумкин. (ЧДК) усули қурилиш тамойили чизиқли криптоанализ (ЧК) ҳамда дифференциал криптоанализ (ДК) усулларини умумлаштиришга асосланган бўлиб, Фейстел тармоғига асосланган n раундли шифрлаш алгоритми учун унинг умумий қўлланилиш схемаси 1.5-расмда келтирилган. [14]



1.5-расм. ЧДК усулининг умумий қўлланиш схемаси

Яъни, криптоанализнинг дастлабки қадамида кирувчи (1-раундга кирувчи) айирмани билган ҳолда m - раунддан чиқувчи айирма қиймати ДК усули орқали аниқланади, кейинги қадамда $n-1$ -

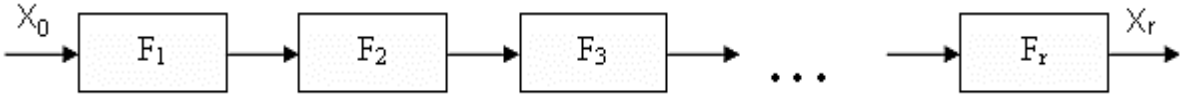
раунддан чиқувчи айирма қиймати ЧК усули орқали аниқланади. Сўнгги қадамда эса охирги раунд функциясига кирувчи ва функциядан чиқувчи айирма ва шифр матн қийматларини билган ҳолда сўнгги раунд функциясида фойдаланилган калит вариантлари статистика ўтказиш (текшириб кўриш) орқали аниқланади.

Криптоанализ самарадорлиги ҳам айнан ДК ва ЧК усуллари самарадорлигига яъни, улар орқали аниқланган сўнгги раунд функциясидан чиқувчи айирма қийматининг тўғри аниқланганлигига боғлиқдир.

Слайдли ҳужум криптоанализ усули асосан Фейстел тармоғига асосланган шифрлаш алгоритмларига қаратилган. Агар Фейстел тармоғи бўйича қурилган шифрлаш алгоритмларининг киришига n битли маълумот келиб тушадиган бўлса, унда қисм калитнинг узунлиги $n/2$ битни ташкил қилади. Шу боис ҳам шифрлаш алгоритмида фойдаланилган махфий калитнинг узунлиги $n/2$ ни ташкил этади.[13].

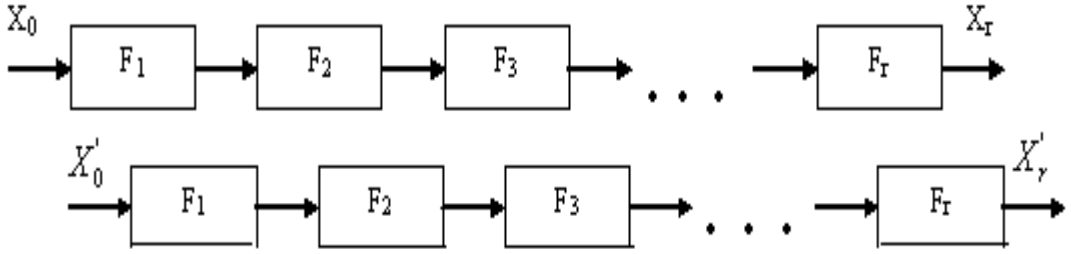
Қуйида келтирилган 1.6-расмда n битли x_0 очиқ матнни шифрлаш жараёни кўрсатилган, унинг натижасида x_r шифрматн ҳосил бўлади. Бу ерда x_j j-чи раундан кейинги берилганларнинг оралиқ қийматини белгилайди, $x_j = F_j(x_{j-1}, k_j), j = 1,2,3,...,r$.

Кейинчалик, баъзан F функцияни белгилашда k қийматни тушуриб қолдирамиз $F(x,k)$ ёки $F_j(x,k)$ ўрнига $F(x)$ ёки $F_j(x)$ деб ёзиш мумкин.



1.6 - расм. Оддий блокли шифрлаш алгоритми схемаси.

Таъриф. F функция “кучсиз” деб аталади, агар маълум $F(x_1,k)=y_1$ ва $F(x_2,k)=y_2$ икки тенгликда k калитни аниқлаш осон бўлса қуйидаги 1.7- расмда бундай турдаги шифрлаш алгоритмлари учун слайдли ҳужумни қўлланилиши мумкинлиги кўрсатилган.



1.7- расм. Оддий слайдли ҳужум схемаси.

Слайдли ҳужум усулининг ғояси шундаки, жараёнлардан бири иккинчисидан бир раундга кечиктириб, иккита шифрлаш жараёнини ўзаро мос қўйиш асос қилиб олинади. Шундай қилиб, жараёнлардан бири иккинчисидан бир раундга ортда қолади. [14]

Айтайлик, x_0 ва $x_0^{'}$ бошланғич очиқ матнлар ва уларнинг мос кетма-кетликлари $x_j=F_j(x_{j-1})$ ва $x_j^{'}=F_j(x_{j-1}^{'}), j=1,...,r$ берилган бўлсин.

*Тасдиқ*_Агар $x_1=x_0^{'}$ қийматлар жуфтлигига эга бўлинса, у ҳолда уларга мос $x_r=x_{r-1}^{'}$ қийматлар жуфтлигига ҳам эга бўлинади.

Айтайлик, $(P,P^{'})$ - очиқ матнлар, $(C,C^{'})$ - эса уларга мос шифрматнлар берилган бўлсин.

Таъриф (P,C) *ва* $(P^{'},C^{'})$ жуфтлик слайд жуфтлик дейилади, агар қуйидаги шартлар бажарилса [1,2,4]:

– $F(P)=C$, $F(P')=C'$

– $C=P'$

– $F(P)=P'$, $F(C)=C'$

Агар P очиқ матн F функциядан ўтказилгандан кейинги натижаси C шифрматнга , P' очиқ матн F функциядан ўтказилгандан кейинги натижаси C', ҳамда биринчи очиқ матнни шифрлаш натижаси, яъни C шифрматн, иккинчи очиқ матн P' га, яъни $C=P'$ тенг бўлса, у ҳолда $F(P)=P'$, $F(C)=C'$ бўлади.

Слайдли ҳужум криптоанализ усули қуйидаги тарзда амалга оширилади. Бунинг учун, $2^{n/2}$ жуфт (P_i,C_i) очиқ-ёпиқ матнлар жуфтлигини оланади ва уларнинг орасидан слайдли жуфтликлар қидирилади. Топилган очиқ-ёпиқ матнлар орасидан “Туғилган кунлар” парадоксига кўра ҳеч бўлмаганда бир жуфт шундай (i,i') индекслар топиладики, қандайдир қисм калит учун $F(P_i)=P'_i$ ва $F(C_i)=C'_i$ тенгликлар бир вақтда бажарилади. Слайдли жуфтлик топилгандан сўнг, қисм калитнинг маълум бир битларини топиш мумкин .

Алгебраик криптоанализ (АК) усулининг моҳияти шифрлаш алгоритмини ифодаловчи чекли майдонда аниқланган алгебраик тенгламалар системасини тузиш ва шу тенгламалар системасини ечиш орқали шифрлаш калитини топишдан иборат .

АК усули очиқ ва шифр матн асосидаги ҳужум турига тегишли бўлиб, унинг мураккаблиги мумкин бўлган барча ТС куриш ва ечиш ҳисобланади. Шунинг учун АК жараёнида алгебраик чизиқсизлик даражалари паст тенгламала системасини куриш ва уларни ечишнинг оптимал йулларини топиш муҳим саналади.

Криптоанализнинг шифрлаш алгоритмини тенгламалар системаси орқали ифодалаш босқичи қўйидаги қадамлар асосида амалга оширилади:

a) *шифрлаш алгоритмини декомпозициялаш*; яъни, шифрлаш алгоритмининг ташкил этувчиларини имкон қадар кичик ва алоҳида элементлар (чизиқли, чизиқсиз ва бошқа акслантиришлар)га ажратиш.

b) *ҳар бир элементни алгебраик ифодалаш*; яъни, ҳар бир акслантириш учун, уларни кириши ва чиқишини боғловчи имконият даражасида минимал алгебраик чизиқсизлик даражасига эга бўлган ТС ҳосил қилинади. Бир турга мансуб бўлган акслантиришлар учун ТС ҳосил қилиш бир хил тарзда амалга оширилади. Мазкур ТС фақат номаълумлари билан фарқланади.

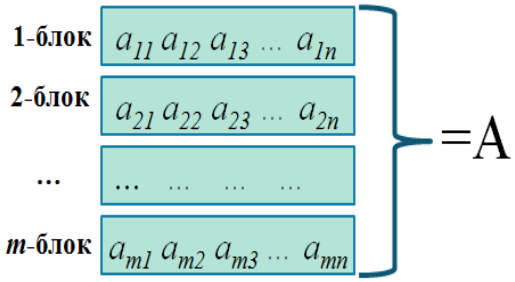
c) *ҳар бир элементнинг кириши ва чиқишини бошқа элементлар ҳамда калит, очиқ матн ва шифр матн битлари билан боғлаш*.

Таъкидлаш лозимки, ТС қуриш жараёни таҳлил қилинаётган шифрлаш алгоритми тузилиши ва унинг ташкил этувчи элементлари хусусиятларига боғлиқ ҳолда амалга оширилиб, ихтиёрий шифр учун ТС қуришнинг универсал ва оптимал ечими мавжуд эмас. Бироқ бугунги кунда чекли майдонда аниқланган чизиқсиз тенгламалар системасини ечишга қаратилган кўплаб усуллар (масалан: Бухбергер, F4, F5, F5C, G2V, GVW, SAT-solvers, XL, XL2, XLF, XSL, FXL, XFL, WXL, HXL, MutantXL ва MXL2) таклиф этилган ва улардан АК ўтказишда бевосита фойдаланиб келинмоқда.

Интеграл криптоанализ усулини бирор-бир блокли симметрик шифрлаш алгоритмига қўллаш учун, танлаб олинган очиқ матнлар ва

уларга мос шифрматнларнинг махсус тўплами ҳамда шифрлаш алгоритми маълум бўлиши лозим.

Криптоанализ учун очиқ матнлар тўпламини (А) танлаш қуйидаги тартибда амалга оширилади (1.8-расм).



1.8-расм. Очиқ матнлар тўплами

Ушбу расмда, m – танлаб олинувчи блоклар сони ва $m = 2^N, N$ – a_{ij} элементни битлар сони, n – қаралаётган алгоритм кирувчи блок узунлигига боғлиқ.

Ушбу А – очиқ матнлар тўплами қуйидагича аниқланувчи *актив* ва *пассив* элементлардан ташкил топиши керак, яъни:

– Агар $j = 1..n$ учун $a_{1,j} \neq a_{2,j} \neq a_{3,j} \dots \neq a_{m,j}$ бажарилса, очиқ матнлардаги $\mathrm{a_{i,j}(i = 1 \dots m, j = const)}$ элементлар *актив элементлар* ҳисобланади;

– *Агар* $j = 1..n$ *учун* $a_{1,j} = a_{2,j} = a_{3,j} \dots = a_{m,j}$ *бажарилса, очиқ матнлардаги* $a_{i,j}$ *(i=1 ...m, j=const) элементлар пассив элементлар ҳисобланади.*

1. *Теорема*. Ушбу танлаб олинган А – очиқ матнлар тўплами элементлари учун қўйидаги тенглик ўринли:

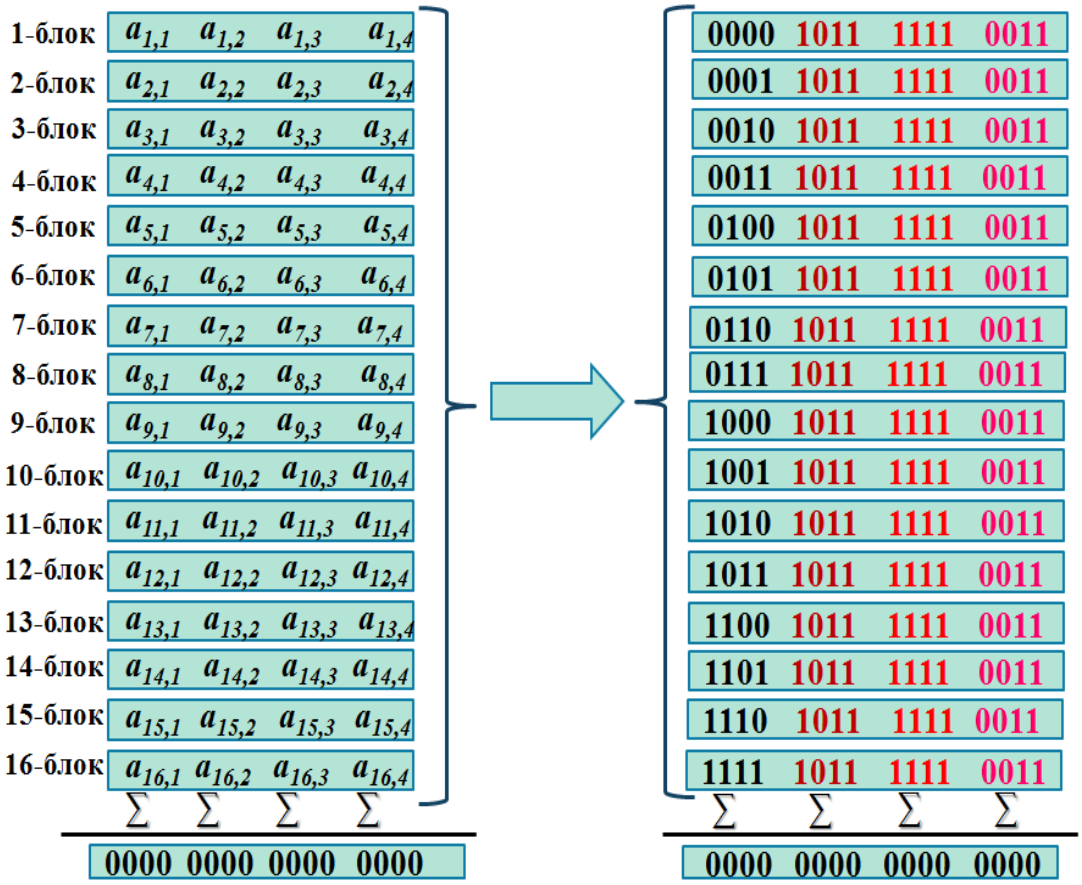
$$\sum_{i=1}^{m} a_{ij} = 0$$

бу ерда $j = 1,2,3, \dots, n$.

Очиқ матнлар тўпламини танлаб олишни қуйидаги мисолда кўришимиз мумкин.

Айтайлик a_1, a_2, a_3, a_4 – бирор шифрлаш алгоритми учун кирувчи блок ҳамда $\boldsymbol{a_i}$ – ярим байт (битлар сони 4 та) бўлсин, у ҳолда танлаб олинувчи блоклар сони 16 та ($m = 2^4 = 16$) бўлади.

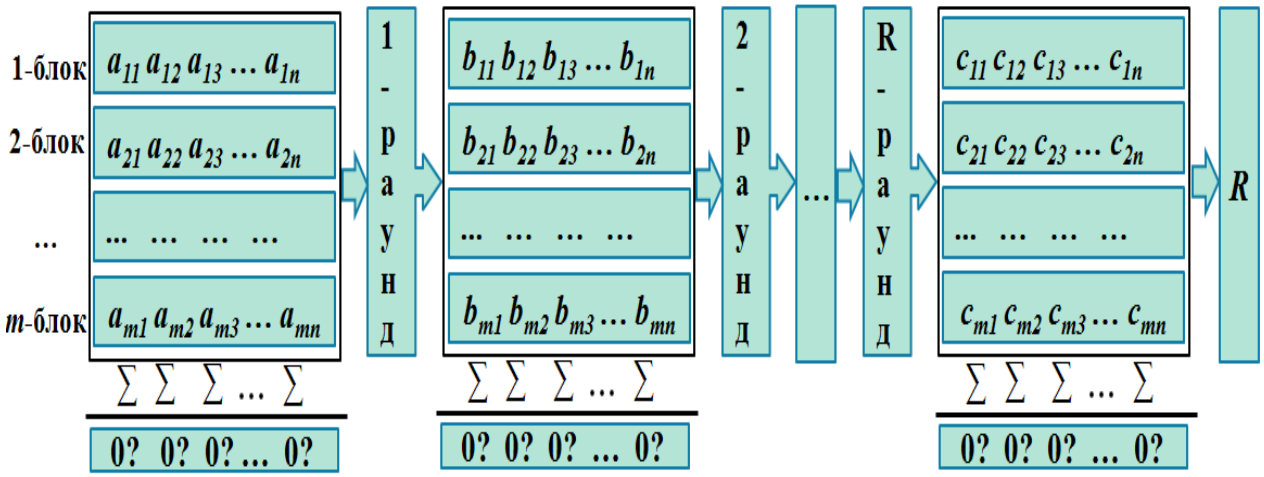
Ушбу блокларни юқоридаги талаблар асосида қуйидагича шакллантириш мумкин (1.9-расм):



1.9-расм. Очиқ матнлар тўплами.

Ушбу танлаб олинган очиқ матнлар тўплами учун юқоридаги теорема шартлари қаноатлантиради. Яъни, ҳар бир очиқ матнлар блокининг мос элементлари йиғинидиси (*XOR*) нолга тенг бўлади. Шунингдек, ушбу очиқ матнлар тўпламида мос равишда биринчи элементлари актив, қолган элементлари эса мос равишда пассив элементлар ҳисобланади.

Криптоанализ жараёнида, танлаб олинган А тўплам хусусиятининг шифрлаш алгоритми раундларидан ўтганда қандай ўзгариши бўйича тадқиқот олиб борилади (1.10 -расм). Агар кузатилаётган очиқ матнлар тўпламининг бирор R-раунддан чиқиш холатида баланслашганлик хусусияти бузулиб, ҳамда актив ёки пассив байтлар мавжуд бўлмаса, у ҳолда R раундли шифрлаш алгоритмининг сўнги раундида фойдаланилган махфий калитни топиш имконияти туғилади. [15,17,19]

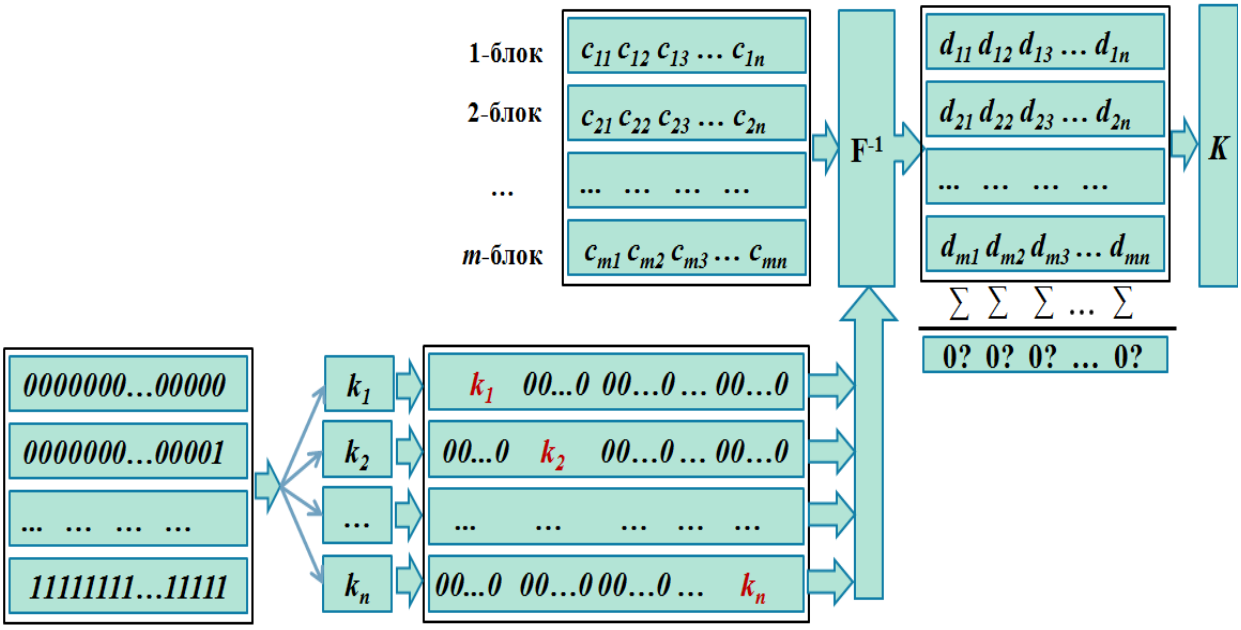


1.10-расм. Очиқ матнлар тўпламини кузатиш схемаси.

Демак, очиқ матнлар тўпламини кузатишда актив ёки пассив байтларнинг мавжудлиги қанчалик кўп раундда сақланиб, баланслашганлик хусусияти бажарилса, шифрлаш алгоритмининг интеграл криптоанализ усулига криптобардошлиги ҳам шу қадар паст бўлади.

Шифрлаш алгоритмининг сўнги раундида фойдаланилган калит қийматини аниқлаш эса, сўнги раундга кирувчи тўпламда актив (ёки пассив) байт мавжудлигини ҳамда сўнги раунддан чиқувчи маълумотни билган ҳолда, статистика ўтказиш йўли орқали амалга

оширилади. Қуйидаги 1.11-расмда, ушбу жараённи амалга оширишнинг функционал схемаси келтирилган.



1.11-расм. Калит қийматини аниқлашнинг функционал схемаси

Яъни, танлаб олинган очиқ матнларга мос шифр матнларни бирор танлаб олинган калит асосида бир раунд дешифрлаймиз. Агар дешифрлашдан ҳосил бўлган матнлар учун юқоридаги теорема шарти бажарилса, ушбу калит номзод калитлар рўйхатига қўшилади. Ушбу жараён, барча танлаб олинган калитлар устида амалга оширилади.

Айни вақтда стандарт шифрлаш алгоритмлари мухим камчиликларидан бири уларнинг реал техник криптоанализ усулларига нисбатан бардошсиз эканлигини кўрсатмоқда, хусусан “аппарат хатоликларини генерациялашга асосланган криптоанализ” усулларига. Бу усулнинг моҳияти, алгоритм акслантиришларининг маълум жойларидаги айрим битларини ўзгартиришга эришиш мақсадида, ҳимоя аппаратига иссиқлик, юқори частотали, ионизациялаш ва бошқа ташқи таъсир усулларидан фойдаланган ҳолда таъсир этишдир. Бундай ўзгартириш киритишга асосланган таҳлил

усули маълумотни ўзгартириш киритилгунга қадар ва ўзгартирилганидан сўнг эга бўлган маълумотларини солиштириш орқали охирги раунд калити ва кейинчалик барча раунд калитлари тўғрисида қийматлар топишга қаратилган. [13,65]

1.3. Асимметрик шифрлашларнинг бардошлигини аниқлаш усулларининг тадқиқи

Маълумки, энг кўп фойдаланиб келинган носимметрик тизимларга бардошлилиги учта муаммонинг, яъни факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш мураккаблиги муаммоларидан бири билан белгиланадиган криптотизимлар киради. Булар билан бир қаторда қўшимча махфийликка эга бўлган носимметрик криптотизимлар ҳам юзага келмоқда. Улар криптотизим яратувчи криптографлар учун ҳам, криптотизимни қўпоришни ёки ҳужум учун бардошлиликни баҳолашни мақсад қилган субъектларга криптотаҳлил объекти бўлиб хизмат қилади.

Дискрет логарифмлаш муаммосининг мураккаблигига асосланган носимметрик криптотизимлар криптотаҳлили. Дискрет логарифмлаш усуллари ва кейинги параграфда кўриладиган факторлаш усуллари орасида параллеллик - ўзига хос изоморфизм мавжуд. Масалан, Диксон алгоритми билан индексли ҳисоблаш алгоритмлари бир-бирига жуда ўхшаш, иккала алгоритмда ҳам тенгламалар системасини тузиш ва чизиқли алгебрадан фойдаланиш босқичлари ўхшаш. Лекин, дискрет логарифмлаш муаммоси факторлаш муаммосига нисбатан мураккаброқдир. Агар дискрет логарифмлашнинг полиномиал алгоритми яратилса, унда факторлаш муаммоси ҳам осон ҳал бўлади.

Ҳозирги кунда энг самарали ҳисобланган криптотаҳлил алгоритмлари субэкспоненциал мураккабликка эгадир. Бу алгоритмлар “index-calculus” (индексли ҳисоблаш) алгоритмлари бўлиб, фактор базасини қуришга асосланган. [12,20]

Туб майдонда дискрет логарифмлаш учун биринчи субэкспоненциал алгоритм Леонард Адлеман томонидан таклиф этилган. Бироқ амалиётда бу алгоритм етарли даражада самарали бўлиб чиқмаган. Дон Копперсмит, Эндрю Одлижко ва Ричард Шреппель дискрет логарифмлаш учун “COS” номи остида субэкспоненциал алгоритмнинг ўз русумларини таклиф этдилар. Оливер Широкаур томонидан таклиф этилган сонли майдон ғалвири алгоритми $p > 10^{100}$ бўлганда COS алгоритмининг барча модификацияларига нисбатан самаралироқ ишлайди. Сонли майдон умумлашган ғалвир усулининг мураккаблиги $C = O(exp(c(\ln p)^{\frac{1}{3}}\ (ln\ ln\ p)^{\frac{2}{3}}))$амал билан баҳоланади, бу ерда c≈1,92.

Фараз қилинсинки, G - мультипликатив Абель группаси бўлсин. a асос бўйича дискрет логарифм b ни ҳисоблаш, шундай $x \in G$ ни топишга келтириладики, $a^x = b$ бўлсин. Дискрет логарифмнинг хоссалари ҳақиқий сонлар майдонидаги одатдаги логарифм хоссаларига кўп жиҳатлардан ўхшаш. Масалан,

$$log_a\ (h * j) \equiv\ log_a\ (h) +\ log_a\ (j)\ (mod\ \left|G\right|)$$

кўринишдаги айният кучга эга, бу ерда $\left|G\right|$ - группанинг тартиби, a -ҳосил қилувчи (генератор). Индексли ҳисоблаш усулининг асосий ғояси шундаки, агар чекли майдон Z_pнинг баъзи элементлари учун

$$\prod_{i=1}^{m} x_i \equiv \prod_{j=1}^{m} y_j$$

бўлса, унда

$$\sum_{i=1}^{m} log_a x_i \equiv \sum_{j=1}^{m} log_a y_j mod\ (p-1).$$

Охирги таққосламалардан бир қанчасини ҳосил қилингач, $log_a x_i$ ва $log_a y_j$ номаълумларга нисбатан чегирмалар ҳалқаси Z_{p-1} да унча кўп номаълумларга эга бўлмаган тенгламалар системасини тузиш ва ҳал этиш мумкин. Шуни унутмаслик керакки, охирги таққосламада, ҳеч бўлмаганда $log_a g$ қиймати маълум бўлган битта элемент g қатнашиши шарт.[19,21]

Охирги таққосламани генерация қилишнинг энг осон усули, бу бирор $g \in Z_p$ ни танлаш, $u=a^g \ (mod\ p)$ ҳисоблаш ва кетма-кет танлаш усулида

$$u=\prod_{i=1}^{k} p^{\alpha i}{}_i$$

муносабатни қаноатлантирувчи сонларни топишдир. Бу ерда p_i - B дан кичик туб сонлар. Агар шундай сонларни топишнинг иложи бўлса, унда u силлиқлик чегараси B га эга бўлган силлиқ элементдир.

Дискрет логарифмлаш алгоритмида ҳам факторлаш алгоритмига ўхшаш икки босқич кўзга ташланади:

- биринчи, тайёрланиш босқичида бирор чегара B танланади ва фактор базаси ва бу база асосида тенгламалар системаси шакллантирилади;

- иккинчи босқичда тенгламалар системасининг ечими топилади.

Шундай қилиб, дискрет логарифмлашнинг барча усуллари ҳам охир оқибатда тенгламалар системасини ҳал қилишга келтирилади.

*Факторлаш муаммосининг мураккаблигига асосланган носимметрик криптотизимларнинг криптотаҳлили***.** Факторлаш

муаммосининг юзага келиши антик даврларга, Эратосфен яшаган даврларга, тахминан, эрамизгача 284-202 йилларга тўғри келади, муаммонинг ундан кейинги тарихи Фиббаночи (тахминан 1180-1250 йй.), Ферма (1601-1665 йй.), Эйлер (1707-1783 йй), Лежандр (1752-1833 йй.), Гаусс (1777-1855 йй.) каби улуғ математиклар номи билан боғланган.[21,23]

Факторлаш муаммосини ҳал этишда n модулни факторлаш масаласини ечишда биринчи навбатда ҳаёлга келадиган усул, бу $\sqrt{n}$ дан ошмайдиган туб сонларни танлаб уларга бўлиб кўришдир. Бошқа танлаш усули Фермага тегишли бўлиб, n ни квадратлар айирмаси кўринишида ифодалашга асосланган:

$$n = a^2 - b^2 = (a + b)(a - b).$$

Ферма энг катта умумий бўлувчи - $EKUB(n, a-b)$ ни, яъни n нинг нотривиал бўлувчисини топишга ҳаракат қилишни ҳамда бунга имкон берувчи усулни ҳам таклиф этган. Агар n нинг кўпайтувчилари бир-биридан катта фарқ қилмаса, бу усул оддий танлаш усулига нисбатан тез ечим беради ва унинг мураккаблиги $O(\sqrt{n})$ кўринишида ифодаланади, аммо ҳозирги кунда криптографик тизимларда амалда фойдаланиладиган ҳоллар учун аҳамиятга эга эмас. Лежандр мазкур ёндашувда $a^2 \equiv b^2 \pmod{n}$ га эга бўлиш лозимлигига эътибор қаратган. Аммо, келтирилган таққослама ҳар қандай n учун етарли эмаслигини ҳам кўрсатган ва кўзланган мақсадга эришиш учун узлуксиз касрлардан фойдаланиш йўлини таклиф этган.

Компьютерлар асрида дастлабки 1970 йилларда таклиф этилган факторлаш алгоритмларидан бири $(p-1)$ Поллард алгоритми бўлган. Ундан сўнг $(p+1)$ Вильямс алгоритми ва ЭЭЧлардан фойдаланишга

асосланган Ленстра алгоритми ишлаб чиқилди. Кейинчалик *(p-1)* Поллард алгоритми *(p+1)* Поллард алгоритми сифатида, Поллард r -, λ - усули номлари остида такомиллаштирилди. r - λ - Поллард усулининг мураккаблиги $I_p = \sqrt{\pi q/4}$ амал билан белгиланади. Ҳозирги кунга келиб, факторлаш муаммосининг энг тезкор усуллари бўлиб, чизиқли ғалвир, квадратик ғалвир, сонли майдон ғалвири, умумлашган сонли майдон ғалвири усуллари тан олинган.[26]

Ҳозирги кунда энг самарали криптотаҳлил алгоритмларининг мураккаблиги экспоненциал эмас, балки субэкспоненциал мураккабликка эга.

Алгоритм экспоненциал мураккабликка эга дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(t^{f(n)})$ бўлса.

Алгоритм полиномиал мураккабликка эга дейилади, агарда унинг мураккаблиги қийматининг тартиби $O(n^m)$ бўлса. Субэкспоненциал мураккабликка эга бўлган алгоритм мураккаблиги қийматининг тартиби $O(n^m)$ ва $O(t^{f(n)})$ орасида бўлади.

Факторлаш муаммоси асос қилиб олинган RSA алгоритмининг муаллифларидан бири Рональд Райвест 1977 йилда 125 разрядли сонни факторлаш учун 40 квадратиллион йил керак бўлади деб “башорат” қилган эди. Аммо, 1994 йилдаёқ 129 ўнли хонали сон факторланди.

Квадратик ғалвир усули асослари.Факторлашнинг квадратик ғалвир усули Диксон усулига жуда ўхшаш. Иккала алгоритмда ҳам чизиқли алгебра асосларидан бир хил тарзда фойдаланилган. Яъни, аввало чегара B танланади ва B дан катта бўлмаган туб сонлардан фактор базаси шакллантирилади. Шаклланган база етарли миқдорда B-силлиқ сонларни ўз ичига олиши шарт.

Кейин кўпҳад $Q(x)=(\lfloor\sqrt{n}\rfloor+x)^2+n$ аниқланади. Бу кўпҳад квадратик бўлиб, база элементларини *B*-силлиққа текшириш учун фойдаланилади. Усул номида “квадратик” атамаси қатнашиши кўпҳад квадратик бўлганидан келиб чиққан.

Силлиқлик муносабатига эга бўлган сонларни танлаш учун *0* сонини ўз ичига олган интервал, масалан, *[-M; M]* дан ҳар бир бутун сон $x\in[-M;M]$ учун $y=Q(x)$ ҳисобланади. Сўнгра *n* модуль бўйича $y=\underline{x}^2$ ҳисобланади, бу ерда $\underline{x}=\lfloor\sqrt{n}\rfloor+x$. Натижада Диксон алгоритмидаги каби *y B*-силлиқми ёки йўқлиги аниқланади. Агар *y* силлиқ бўлса, унда чизиқли тенгламалар системасини ечиш босқичи учун *2* модуль бўйича экспонента сифатида сақлаб қўйилади. Квадратик ғалвир усулининг Диксон усулига нисбатан устунлиги [1, 33] да баён этилган ғалвир тузиш усули билан белгиланади. Ғалвир тузиш фактор базасини шакллантириш ишини осонлаштиради.[42,72]

Қуйида квадратик ғалвир усулининг 1991 йилда таклиф этилган такомиллаштирилган Померанц усулининг асосий ғояси ҳақида тўхталамиз.

Фактор базаси сифатида қандайдир параметр билан чекланган *s* та шундай туб сон p_i лар танланадики, $(n/p_i)=1$ бўлсин, бу ерда (n/p_i) Якоби белгиси.

$m=\lfloor\sqrt{n}\rfloor$, $Q(t)=(t+m)^2-n=H(t)^2$, бу ерда $H=t+\lfloor\sqrt{n}\rfloor$. *t* нинг деярли кичик қийматларида $Q(t)$ нинг қиймати ҳам катта бўлмайди. Кейинги қадамда, *t* сонларини кўриб чиқиш ва $Q(t)$ ларни кўпайтувчиларга ажратиш ўрнига, алгоритм биратўла “кераксиз” *t*

ларни чиқариб ташлайди ва фактор базаси орасида фақат $Q(t)$ нинг бўлувчилари мавжуд бўлганларини қолдиради, яъни

$$A=Q(t)= \prod_{j=1}^{s} p_j^{\gamma_j},$$

$Q(t)$ фактор базасида ажратилади. Унда $B=H(t)$ белгилаш орқали $B^2 \equiv A^2 (mod\ n)$ таққосламага эга бўлинади ва бундай таққосламаларни тўплаб, ўзгарувчиларни сафдан чиқариш орқали Диксон алгоритмидагидек $X^2 \equiv Y^2\ (mod\ n)$ таққосламасига эга бўлинади, оқибатда факторлар топилади.

Бугунги кунда сонли майдон ғалвири усули ва Померанцнинг такомиллашган квадратик ғалвир усули энг тезкор усуллардир.

Сонли майдон ғалвири усули асослари. Дастлабки Поллард тезкор факторлаш усули томонидан таклиф этилган бўлиб, махсус кўринишдаги сонларни (масалан, Ферма сонларини) факторлаш (SNFS) учун мўлжалланган. SNFS усулида энг катта факторланган натурал сон *227* ўнли хонали рақамларда берилган сондир. Аммо RSA-модуллари махсус кўринишга эга бўлмаганлиги боис, уларни умумлашган сонли майдон ғалвири (GNFS) усули асосида факторлаш мумкин. Ҳозиргача эришилган рекорд натижалар *155* ўнли хонали (*512* бит) сонлар учун эришилган. Бу сонни факторлаш учун *8400 mips-йил* сарф бўлган.

Ҳозирги кунда сонли майдон ғалвири усули асосида *110* ва ундан ортиқ ўнли хонали узунликдаги модулларни факторлаш учун энг тезкор алгоритмлар ишлаб чиқилган. Квадратик ғалвир усули нисбатан тўппа-тўғри мақсадга элтишга етарли бўлса ҳам, сонли майдон ғалвири усули такомиллашган математик асосларга таяниши билан истиқболлироқдир. Сонли майдон ғалвири ўз моҳияти бўйича

алгоритм эмас, балки бир неча босқичдан таркиб топган алгоритмлар мажмуасидир.[78]

Квадратик ғалвир алгоритмининг мураккаблиги $C_1=O(exp((ln p)^{1/2} (ln ln p)^{1/2}))$ амал билан баҳоланса, сонли майдон ғалвири усулининг мураккаблиги $C_2=O(exp(c(ln p)^{1/3} (ln ln p)^{2/3}))$ амал билан баҳоланади, бу ерда $c\approx1,9223$. Сўнги ифодада $(ln p)^{1/2}$ ҳади $(ln p)^{1/3}$ га айланган, аммо C_2 да нисбатан катта c нинг қатнашиши квадратик ғалвир алгоритми узунлиги *110* ўнли хонали бўлган модуллар қулайлигига сабаб бўлади.

n нинг бинар узунлиги $x=log\ n$ га тенг олиниши келтирилган усул мураккаблилигини симметрик криптотизимлар калит узунлиги бўйича мураккаблиги билан таққослаш имконини беради.

Қуйида келтирилган 1.4-жадвалнинг биринчи устунида усуллар, иккинчи устунида факторлаш учун амаллар сарфи $f(x)$, учинчи устунида $log_2f(x)$ келтирилган.

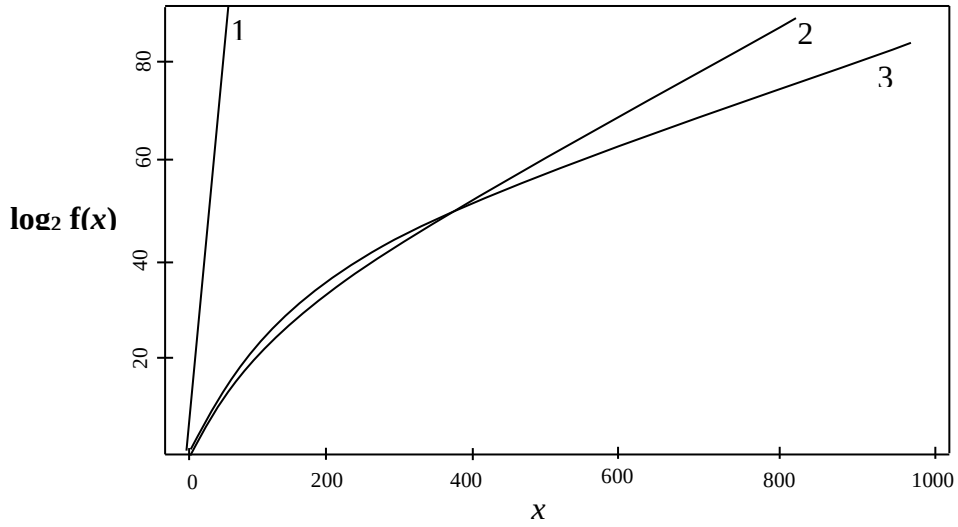
1.4-жадвал

Усуллар мураккаблиги

Усуллар	$f(x)$	$log_2f(x)$
Танлаб бўлиш	$2^x/x$	$x- log_2 x$
Квадратик ғалвир	$2^c (log_2x)^{½}$, бу ерда $c=x^{1/2}$	$x^{1/2} (log_2x)^{1/2}$
Сонли майдон ғалвири	$2^{1.9223d} (log_2x)^{2/3}$, бу ерда $d=x^{1/3}$	$1.9223\ x^{1/3} (log_2x)^{2/3}$

Келтирилган жадвалдан субэкспоненциал мураккабликка эга бўлган квадратик ғалвир ва сонли майдон ғалвири усуллари асимптотик мураккаблик нуқтаи назаридан экспоненциал

мураккабликка эга бўлган алгоритмлардан устунлиги билан белгиланиши, бироқ полиномиал мураккабликка эга алгоритмлар билан рақобатлаша олмаслиги аён бўлади. 1.12-расмда танлаб бўлиш (1), квадратик ғалвир (2) ва сонли майдон ғалвири (3) усуллари бўйича тузилган алгоритмлар мураккабликларининг *x,* яъни модуль бинар узунлигига нисбатан ўзгариш графиги келтирилган. Шуни қайд этиш лозимки, квадратик ғалвир усули сонли майдон ғалвири усулидан *390* битли модулларни факторлашда мураккаблик бўйича устунликка эга. Шунингдек, 4-расм асосида симметрик алгоритмлар шифрлаш калити узунлигига мос факторлаш мураккаблигини берувчи RSA алгоритми модулининг битлар сонини аниқлаш мумкин. Масалан, *390* битли RSA-модулни факторлаш *60* битли симметрик тизим шифрлаш калитини топиш мураккаблигига тенг.



1.12-расм. Факторлаш алгоритмлари мураккабликларини таққослаш

Бу усул барча ҳозиргача маълум бўлган бошқа криптоанализ усулларини сиқиб чиқарган. NFC усули асосида криптоанализ учун зарур амаллар бажариш вақти қуйидаги ифода бўйича аниқланади:

$$T = e^{c},$$

бу ерда

$$C=((1.923+O(1)*(Ln(n))^{1/3}*(Ln(Ln(n)))^{2/3}.$$

Ҳисоблашлар тезлиги 10^6 бўлган компьютердан фойдаланиб амалга оширилганда C ифодасида $O(1)=1$ учун амаллар бажариш вақти *1 мс* га тенг. NFC усулининг истиқболдаги тараққиёти *1.923* доимийсини камайиши йўналишида юз бериши башорат қилинган. Кўпгина махсус тузилмали сонлар, масалан, Ферма сонлари учун доимий *1.5* гача камайиши маълум. Ҳозирги кунда қўлланиладиган факторлаш қийин бўлган модуллар криптоалгоритм яратиш жараёнида аниқ белгилаб қўйилган талабларга жавоб бериши шарт. Бу талаблар жумласига махфий даража кўрсаткичи d нинг катта сон бўлиши, ошкора калит қисми $e > 3$ шартига жавоб бериши, махфий туб модуллар учун $p-1$ ва $q-1$ ларнинг факторлари катта туб сон бўлиши ва шунга ўхшаш. Агар бундай модуллар учун ҳам доимийни *1.5* га камайтириш йўли топилса, унда *1024* битли сонларни ҳам мавжуд ҳисоблаш техникаси даражасида факторлаш мумкин бўлар эди. Доимийни камайтириш усулларидан бири бўлиб кўпҳад кўринишидаги сонларни кичик коэффициентлар орқали ифодалаш усулини топиш ҳисобланади. Ҳозирча адабиётларда бундай усул мавжудлиги ҳақида ахборот берилмаган.

Боб бўйича хулоса

Хулоса қилиб айтганда, ушбу бобда криптография ва криптотаҳлил соҳасининг сўнгги йигирма йиллик ривожланиш тенденциялари, замонавий шифрлаш алгоритмларининг чидамлилик даражаси ва уларга нисбатан қўлланиладиган ҳужум турлари тизимли равишда тадқиқ этилди. Олиб борилган изланишлар натижасида қуйидаги илмий ва амалий хулосаларга келинди:

Классик ва замонавий криптотаҳлил усуллари: Криптографик алгоритмларни таҳлил қилишнинг фундаментал усуллари, жумладан, калитни тўлиқ танлаш (brute-force), частотавий таҳлил ва калит генераторларининг статистик хоссаларини ўрганиш масалалари кўриб чиқилди. Шунингдек, мураккаб алгоритмларга нисбатан Поллард усули, «ўртада учрашиш» (meet-in-the-middle) ҳамда коллизия ҳодисаларини келтириб чиқариш орқали шифрни бузиш имкониятлари таҳлил қилинди.

Математик ва алгоритмик ҳужумлар: Симметрик блокли шифрларга нисбатан энг хавфли ҳисобланган *дифференциал* ва *чизиқли* криптотаҳлил усулларининг ишлаш принциплари ва уларнинг алгоритм ички структурасига (S-блокларга) боғлиқлиги аниқланди. Бу усуллар шифрнинг математик заифликларини топишда асосий восита бўлиб хизмат қилиши кўрсатиб ўтилди.

Ён канал ҳужумлари (Side-Channel Attacks): Замонавий криптотаҳлилнинг энг долзарб йўналишларидан бири бўлган физик ҳужум турлари батафсил таснифланди.

Хусусан:

- **Вақт ва қувват бўйича ҳужумлар**: Шифрлаш жараёнида сарфланадиган вақт ва энергия истеъмолидаги фарқлар асосида калитни тиклаш (SPA ва DPA ҳужумлари);
- **Физик нурланишлар**: Электромагнит нурланиш, шаффоф нурланиш ва акустик тебранишлар орқали маълумотларни масофадан туриб ўқиш имкониятлари;
- **Тизимли ҳужумлар**: Ҳисоблаш хатолари (fault injection) ва кэш хотирасига ҳужум қилиш орқали алгоритмнинг ишлаш мантиғини бузиш усуллари ёритилди.

Криптобардошликни баҳолаш: Охирги йилларда криптографияда эришилган ютуқлар ва янги турдаги ҳужумларнинг пайдо бўлиши алгоритмларни баҳолашнинг анъанавий усуллари етарли эмаслигини кўрсатмоқда. Бу эса криптобардошликни аниқлашнинг янги, автоматлаштирилган ва кўп факторли баҳолаш тизимларини ишлаб чиқиш заруриятини асослайди.[42,72]

Шундай қилиб, биринчи бобда келтирилган таҳлиллар ва ўрганилган ҳужум моделлари монография ишининг кейинги босқичларида симметрик блокли шифрларни баҳолаш мезонларини ишлаб чиқиш ва криптотаҳлил жараёнларини автоматлаштирувчи дастурий мажмуани яратиш учун мустаҳкам назарий пойдевор бўлиб хизмат қилади

II. БОБ. СИММЕТРИК БЛОКЛИ ШИФРЛАШ АЛГОРИТМЛАРИНИ КРИПТОГРАФИК ТАЛАБЛАР БЎЙИЧА БАҲОЛАШ УСУЛЛАРИ

2.1. Шифрлаш алгоритмлари криптобардошлилигига оид заифликлар

Бугунги кунда криптографик алгоритмлар махсус ахборот-телекоммуникация тизимларининг ажралмас қисми бўлиб, улар заифликларини таҳлил этиш – ахборот хавфсизлигини таъминлашда муҳим ташкил этувчилардан бири ҳисобланади. Криптографик алгоритмларга боғлиқ бўлган ҳар қандай заифлик танишиш доираси (ошкоралик даражаси) чекланган ахборотларнинг чиқиб кетишига олиб келиши мумкин.

Криптографик алгоритмларга боғлиқ барча заифликлар қуйидаги синфларга ажратилади:

– фойдаланилган шифрлаш алгоритми криптобардошлилиги билан боғлиқ заифликлар;

– шифрлаш алгоритмидан нотўғри фойдаланиш (реализацияси) билан боғлиқ заифликлар;

– криптографик тармоқ протоколлари заифликлари.

Амалда кенг қўлланилувчи блокли шифрлаш алгоритмлари криптобардошлилиги билан боғлиқ заифликлар бевосита замонавий ахборотни ҳимоялаш криптотизимларининг муҳим заифликлари ҳам ҳисобланади.

Блокли шифрлаш алгоритмларини криптотаҳлил қилишдаги асосий ва дастлабки маълумотлар алгоритмнинг ўзига хос хусусиятларидир. Шифрлаш алгоритмини билган ҳолда, шифр модели ишончлилигини текшириш учун лозим бўладиган маълумотларни

мустақил тарзда аниқлаш (генерация қилиш) мумкин.

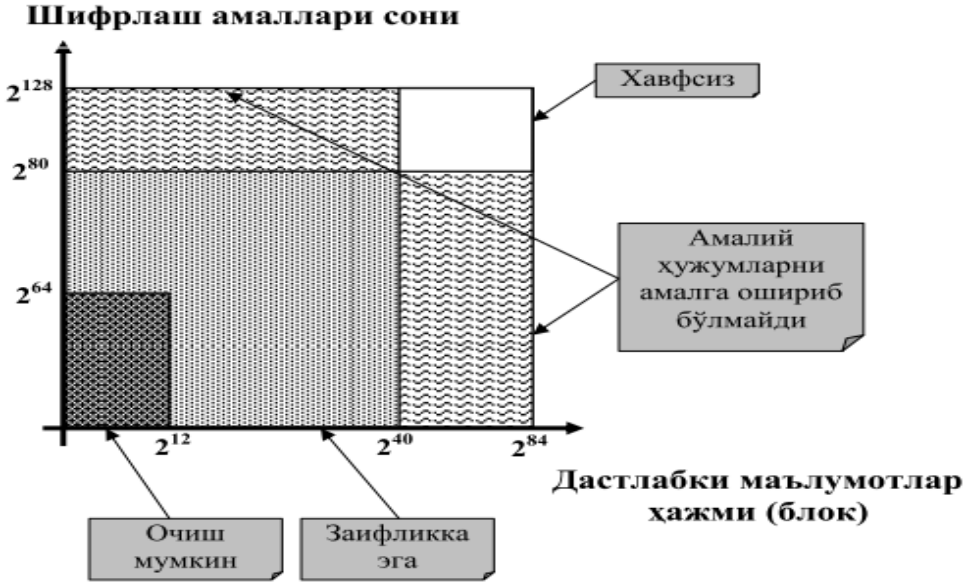
Аниқ бир усул ва уларнинг тегишли параметрларига асосланувчи криптотаҳлил натижаси шифрлаш алгоритмининг хусусий модели (математик, эҳтимолий ва ҳ.к.) ҳисобланиб, ушбу криптотаҳлил усулини амалиётда қўллаш имкониятлари бўйича хулоса бериш учун асос бўлади. Криптотаҳлил ўтказишда лозим бўлган дастлабки маълумотлар (очиқ ёки шифр матн) ҳажми ва кўриниши, шунингдек ҳисоблаш ресурслари ҳажми моделнинг муҳим параметрлари ҳисобланади.

Бугунги кунда замонавий ЭҲМ имкониятлари, талаб этувчи дастлабки маълумотлар ва ҳисоблаш ресурсларига кўра ихтиёрий криптотаҳлил усулининг амалий аҳамиятини 2.1-расмда тасвирланган график асосида баҳолаш мумкин. Шуни ҳам таъкидлаш лозимки, ЭҲМ имкониятларининг ошиши 2.1-расмда тасвирланган соҳалар кўламининг кенгайишига ҳам олиб келади.

Блокли шифрларга қўлланилувчи ихтиёрий криптотаҳлил усули натижасига таъсир этувчи асосий омиллардан бири, бу шифрда фойдаланилган махфий калит ўлчами (узунлиги) ҳисобланади. Шунга мувофиқ, шифрлаш алгоритмлари муаллифлари томонидан шифр махфий калит ўлчами айнан ЭҲМ (техник қурилмалар) ва замонавий криптотаҳлил имкониятларига боғлиқ тарзда ўрнатилади. Калит ўлчамининг етарлича катта бўлиши шифр бардошлилиги ошишига олиб келиши мумкин. Бироқ унинг дастурий ёки аппарат реализациясини қийинлаштиради ва аксинча калит ўлчамининг кичик бўлиши шифр дастурий ёки аппарат реализациясининг осон бўлишига

хизмат қилган ҳолда бардошлиликни тушиб кетишига олиб келади. [44]

Мазкур ҳолат шифрлаш алгоритмини билган ҳолда шифрматнни барча мумкин бўлган калитлар билан дешифрлаб чиқишга асосланган «*Калитларнинг барча мумкин бўлган вариантларини танлаш*» усулига бардошсиз бўлишига олиб келиши мумкин. Мисол учун шифрлаш алгоритми калит узунлиги 100 бит бўлса, барча калит вариантлари сони 2^{100} га тенг, яъни калитлар тўплами қуввати $|K|=2^{100}$. DES шифрлаш алгоритми калити узунлиги 56 бит бўлиб, барча мумкин бўлган калитлар сони $|K|=2^{56}= 0.5*10^{17}$ га тенг. Бунда, агар ҳисоблаш қурилмаси шифрматнни битта калит билан дешифрлаш учун 10^{-6} секунд вақт сарфласа, 24 соатда барча калитлар билан шифрматнни дешифрлаб чиқиш учун $5.787*10^5$ дона ҳисоблаш қурилмаси керак бўлади.



2.1-расм. Турли криптотаҳлил усуллари амалий қўллаш имкониятларини баҳолаш

Ушбу фикрларга асосланган ҳолда, криптография соҳасидаги

муҳим масалалардан бири таклиф этилаётган шифрлаш алгоритми калит ўлчамининг қандай узунликда бўлиши ҳисобланади. Бугунги кунда ахборот хавфсизлиги соҳасида етакчи институт ва ташкилотлар томонидан мазкур масала ечими бўйича турли тавсиялар (ҳисоблаш усуллари) ишлаб чиқилган. Қуйидаги 2.1-жадвалда, блокли шифрларнинг айрим (математик) криптотаҳлил усулларига криптобардошлилигини ишончли таъминловчи калит узунликлари келтирилган. [48]

2.1-жадвал

Шифр бардошлилигини таъминловчи калит ўлчамлари [20]

Тавсия этувчининг шартли номи (эълон қилинган йил)	**Калит узунлиги (бит)**	**Фойдаланиш даври (йил)**	**Манба**
Lenstra and Verheul Equations (2000)	2074	127	[21]
	2075	128	
	2076	129	
	2078	130	
Lenstra Updated Equations (2004)	2088	127	[22]
	2090	128	
	2091	129	
	2092	130	
ECRYPT-CSA Recommendations (2018)	2028	128	
	2068	256	
	2030	128	[23]

NIST Recommendations (2020)	2030	192	
	2030	256	
ANSSI Recommendations (2014)	2020	100	[23]
	2030	128	
NSA CNSA Suite (2016)	Yuqori darajali xavfsiz	256	[24]
Network Working Group RFC3766 (2004)	2053	128	[25]
	2055	129	
	2056	130	
BSI Recommendations (2020)	2026	128	[26]

Демак, жадвал қийматларидан келиб чиқиб, блокли симметрик шифрлаш алгоритмлари махфий сеанс калитлари 128 бит қийматдан кичик бўлиши тавсия қилинмайди. Бироқ блокли симметрик шифрлаш алгоритмлари сеанс калитининг юқорида келтирилган қийматда бўлиши унинг бардошли бўлиши учун зарурий шарт бўлиб, етарли ҳисобланмайди.

Амалиётда блокли симметрик шифрлаш алгоритми раундида фойдаланилган криптографик акслантиришлар умумий криптографик талабларга мос келмаса, мазкур алгоритм 2^{128} дан кичик мураккабликда тегишли криптотаҳлил усуллари билан заифликлари аниқланиши ёки муваффақиятли очилиши мумкин. Шунинг учун ҳам

замонавий криптотаҳлил фанида янги яратилган блокли симметрик шифрлаш алгоритми мавжуд (чизиқли, дифференциал, чизиқли-дифференциал, слайд, алгебраик, интеграл, аппарат хатоликлар ва бошқа) ва алгоритм хусусиятидан келиб чиқувчи криптотаҳлил усулларига текширилади. Текшириш натижалари бўйича шифрлаш алгоритмига тегишли ўзгартиришлар киритилади ёки бардошлилиги ҳақида хулосалар берилади.

Масалан ахборотни ҳимоялаш қурилмасини яратиш “мухандислик” иши деб қаралса, шифрлаш алгоритмининг криптотаҳлил масаласи эса мураккаб, махсус билимларга эга, юқори малакани талаб этувчи янги илмий масалани ечиш ҳисобланади.

Шунинг учун ҳам блокли симметрик шифрлаш алгоритмларини замонавий криптотаҳлил усулларига бардошлилигини баҳолашдаги текшириш қадамлари ва ҳар-бир криптотаҳлил усули баҳоси бўйича алгоритмнинг умумий криптобардошлилиги, амалда қўлланиши мумкинлиги йўналишида ўқув қўлланма ва тавсияномалар ишлаб чиқиш республикада криптотаҳлил фанидаги долзарб масалалардан бири ҳисобланади.

2.2. Симметрик шифрлаш алгоритмларига нисбатан криптографик ҳужум турлари

Ахборотни муҳофаза қилиш тизимининг бир қисмини ёки бутун тизимни бузишга бўлган муваффақиятли ёки муваффақиятсиз уриниш *ҳужум* деб аталади.

Ҳужумнинг қуйидаги турлари мавжуд:

1. *Актив (фаол) ҳужум* - тизимга ёлғон ахборот ўрнаштириш ёки мавжуд ахборотни ўзгартириш йўли билан қилинадиган ҳужум.

2. *Луғат бўйича ҳужум* - тўғридан-тўғри қилинадиган турли кўринишли ҳужумнинг бири бўлиб, бу ҳужум пайтида махфий сўз (парол)лар қайта сараланади ва/ёки олдиндан тузилган махфий сўзлар рўйхатига мурожаат этилади.

3. *Фақат шифрланган матн бўйича ҳужум* - фақат берилган шифрматнга асосланган криптотаҳлил усули.

4. *Қўпол куч ҳужуми, тўлиқ танлаш* - мумкин бўлган қийматларнинг барчасини ёки салмоқли миқдорини ҳақиқий қиймат топилгунча танлашга асосланган ҳужум.

Ёлғон хабарлар ўрнаштиришга, хабарларни тутиб олиш ва ўзгартиришга, маълумотлар базасидан фойдаланишга, ўз ваколатини кенгайтиришга, ёлғон очиқ калитни ўрнаштиришга, сохта ҳужжатлар тайёрлашга, имзодан бош тортишга ва шу кабиларга уринаётган бузғунчи *актив (фаол)* бузғунчи ҳисобланади.[48]

Криптографик баённомани издан чиқариш бўйича ҳаракат қилмайдиган бузғунчи *пассив (суст)* бузғунчи дейилади.

Ахборотни узатишда, сақлашда ёки қайта ишлашда, рақобатчи олдида муайян фойда олиш ёки унга зиён етказиш мақсадида атайлаб, ахборотни рухсат этилмаган тарзда ўзгартириш *ахборотни сохталаштириш* дейилади.

Дастлабки матнни шифрланган матндан шифрлаш калитини билмасдан туриб тиклаш билан тугайдиган криптотаҳлил жараёни шифрни *калитсиз очиш (кенг маънода дешифрлаш)* деб аталади.

Криптотизимни бузиш деганда маъқул бўлган вақтда замонавий ҳисоблаш воситаларидан фойдаланиб криптотаҳлил масалаларини ҳал этиш усулини топиш тушунилади.

Кейинги ўн йилликлар криптологиянинг барча масалалари бўйича очиқ нашрий ишларнинг кескин ўсиб бориши билан характерланади. Ҳозирги кунда криптотаҳлил энг фаол ривожланаётган тадқиқот соҳаларидан бирига айланиб бормоқда. Бардошлилиги шубҳа остига олинмаган кўплаб криптотизимлар очиб ташланди. Криптотаҳлилчи учун катта қизиқиш уйғотадиган математик усулларнинг катта арсенали яратилди.

1970 йиллар бошида фақат симметрик криптотизим маълум эди. Лекин бу мавзу бўйича очиқ эълон қилинган ишлар жуда кам эди. Унга қизиқишнинг пастлиги қатор сабаблар билан белгиланади.

Биринчидан, тижорат учун мўлжалланган криптотизимларга қаттиқ талаб сезиларли даражада эмас эди.

Иккинчидан, асосий ишлар кўлами ёпиқ эканлиги янги натижа олишни истаган кўплаб тадқиқотчи олимларга қийинчилик туғдирар эди.

Учинчидан, энг аҳамиятли омил шуки, криптотаҳлил илмий фан сифатида шаклланмаган бўлиб, жиддий математик тамойиллар билан бирлашмаган тарқоқ усул ("трюк") лар мажмуи эди холос.

1970 йилларда вазият тамоман ўзгарди. Биринчидан, алоқа тармоқларининг ривожланиши ва компьютерларнинг кундалик ҳаётга кириб бориши туфайли ахборотни криптографик муҳофаза қилиш заруратини жамиятнинг тобора кўпроқ табақалари тушуна бошлади.

Иккинчидан, Диффи-Хеллман томонидан 1976 йилда ошкора (очиқ) калитли криптографиянинг ихтиро этилиши махфийликка бўлган тижорат талабларини қондириш учун замин яратди. Бу билан классик криптографиянинг камчилигини белгиловчи асрлар давомида

ечилмай келган калитларни тарқатиш муаммоси ҳал бўлди. Аслида бу ихтиро илмий ҳамжамиятга катта туртки бўлиб, сифат жиҳатдан янги тадқиқ этилмаган соҳани очиб берди. Бу соҳа тез суръатлар билан ривожланиб бораётган ҳисоблаш мураккаблиги назариясига оид янги илмий натижаларни ишлаб чиқишга замин яратди ва бунинг оқибатида жиддий математикавий тамойилларга асосланган *криптотаҳлил йўналиши илмий фан сифатида* шаклланди.[61]

Шифрлаш криптоалгоритмларига қўйиладиган асосий (биринчи) талабнинг моҳияти шундаки, алоқа канали орқали узатилаётган бирор ахборотнинг маъносини очиш худди шу калит билан шифрланган бошқа ахборотнинг маъносини очишга имкон туғдирмаслиги лозим.

Иккинчи талаб шифрлаш ва дешифрлаш аппаратурасини ишлатиш хусусиятларини назарда тутиш ва оператор ёки махфийлаштирилган ахборотни шакллантиришга аралашиш имкони бор шахслар томонидан йўл қўйиладиган баъзи эркинликларни эътиборга олади.

Криптотаҳлил умумий математик натижалардан фойдаланишга ҳам (масалан, катта сонларни туб кўпайтувчиларга ажратиш RSA криптотизимини очиш учун, дискрет логарифмлаш Эль Гамал тизимини очиш учун), муайян криптоалгоритм учун олинган хусусий ҳол бўйича натижаларга ҳам таяниши мумкин. Қоида тарзида, криптотаҳлил алгоритмлари эҳтимоллик алгоритмларидир.[61].

Қуйидаги 2.2-жадвалда криптотаҳлилчида мавжуд бўлган ахборотга боғлиқ ҳолда амалга оширилиши мумкин бўлган криптотаҳлил турларининг умумлашган рўйхати келтирилган.2.2-жадвал

Криптоҳужум турлари

Криптоҳужум тури	**Криптотаҳлилчига маълум маълумотлар**
Фақат шифрматн бўйича ҳужум	• Шифрлаш алгоритми • Дешифрлаш лозим бўлган шифрматн
Маълум очиқ матн бўйича ҳужум	• Шифрлаш алгоритми • Дешифрлаш лозим бўлган шифрматн • Битта махфий калит билан ҳосил қилинган очиқ (дастлабки, асл) матн ва шифрматнлар мос қисмларининг бир ёки бир нечта жуфтлиги
Танлаб олинган очиқ матн асосидаги ҳужум	• Шифрлаш алгоритми • Дешифрлаш лозим бўлган шифрматн • Криптотаҳлилчи танлаган очиқ матн ва унга мос, махфий калит ёрдамида яратилган шифрматн
Танланган шифрматн бўйича ҳужум	• Шифрлаш алгоритми • Дешифрлаш лозим бўлган шифрматн • Криптотаҳлилчи танлаган шифрматн ва унга мос махфий калит ёрдамида шифри очилган очиқ матн.
Танланган матн бўйича ҳужум	• Шифрлаш алгоритми • Дешифрлаш лозим бўлган шифрматн • Криптотаҳлилчи танлаган очиқ матн ва унга мос, махфий калит ёрдамида яратилган шифрматн • Криптотаҳлилчи танлаган шифрматн ва унга мос махфий калит ёрдамида шифри очилган очиқ матн.

Криптотаҳлил жараёни криптотаҳлилчи эга бўлган маълумотлар асосида олиб борилади. Криптотаҳлилчи эга бўлган маълумотларга кўра криптотаҳлил қуйидаги асосий турларга бўлинади:

1) Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида шифрматнни таҳлил қилиш.

Криптотаҳлилчига фақат шифрматн маълум бўлиб, шифрлаш алгоритми маълум эмас. Калит ва шифрлаш алгоритми ҳақида маълумотга эга бўлиш мақсадида криптотаҳлилчи шифрматн параметрларини яъни, шифрматн алфавити ёки шифр белгиларини шифрматнда такрорланишининг сонли характеристикаларини (частоталарини) аниқлаб, очиқ матн қайси тилда ёзилгани, шифрлаш тури, алгоритмни ва калитни аниқлашга ҳаракат қилади. [35]

2) Калит ҳақида маълумотга эга бўлиш мақсадида шифрматнларни таҳлил қилиш.

Криптотаҳлилчига битта k махфий калит билан шифрланган бир нечта $C_1,\ C_2, \dots, C_i$ шифрматнлар ва шифрлаш алгоритми маълум. Криптотаҳлилчининг вазифаси k калитни тиклаш, яъни битта k калит ва E акслантириш (шифрлаш алгоритми) билан $P_1,\ P_2, \dots, P_i$ – очиқ матнларга мос шифрматнлар $C_1 = E_k(P_1), C_2 = E_k(P_2), \dots, C_i = E_k(P_i)$ маълум бўлса, номаълум бўлган очиқ матнлар $P_1,\ P_2, \dots, P_i$ ва $k-$ калитни топиш ёки $C_{i+1} = E_k(P_{i+1})$ тенгликдан P_{i+1} очиқ матнни топиш.

3) Калит ҳақида маълумотга эга бўлиш мақсадида очиқ матн билан таҳлил қилиш.

Криптотаҳлилчига битта k махфий калит билан шифрланган бир нечта шифрматнлар ва уларга мос очиқ матнлар ҳамда шифрлаш алгоритми маълум. Қуйидаги очиқ матн ва уларга мос келувчи шифрматн жуфтликлари:

$(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3))$,…, $(P_i, C_i = E_k(P_i))$

ҳамда шифрлаш алгоритми маълум бўлганда, k – калитни ёки $C_{i+1} = E_k(P_{i+1})$ тенгликда ноъмалум бўлган P_{i+1} очиқ матнни топиш.

4) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган очиқ матн билан таҳлил қилиш.

Криптотаҳлилчига битта k махфий калит билан шифрланган бир нечта шифрматнлар, шифрлаш алгоритми ва криптотаҳлилчи ўзи танлаб олган очиқ матнлар, яъни ушбу жуфтликлар:

$(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3))$,…, $(P_i, C_i = E_k(P_i)$ маълум, криптотаҳлил натижаларига қулайлик туғдирувчи хусусиятларга эга бўлган: P_1, $P_2, \dots, P_i -$ очиқ матнларни танлаш имконияти мавжуд. Криптотаҳлилчининг вазифаси: $k -$ калитни ёки $C_{i+1} = E_k(P_{i+1})$ тенгликдан P_{i+1} очиқ матнни топиш.[51]

5) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган шифр матнлар билан таҳлил қилиш.

Криптотаҳлилчида битта k махфий калит билан шифрланган бир нечта: C_1, $C_2, \dots, C_i -$ шифрматнларни танлаш ва уларга мос: $P_1 = D_k(C_1)$, …, $P_i = D_k(C_i)$ очиқ матнларни ҳам олиш имконияти мавжуд. Криптотаҳлилчининг вазифаси $k -$ калитни топишдан иборат.

6) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган матнлар ёрдамида таҳлил қилиш.

Криптотаҳлилчига битта k махфий калит билан шифрланган бир нечта шифрматнлар, шифрлаш алгоритми ҳамда криптотаҳлилчи ўзи танлаб олган бир ёки бир нечта очиқ матн ва унга мос шифрматнлар, бир ёки бир неча шифрматн ва уларга мос очиқ матнлар маълум. Демак

$(P_1, C_1 = E_k(P_1))$, $(P_2, C_2 = E_k(P_2))$, $(P_3, C_3 = E_k(P_3))$,…, $(P_i, C_i = E_k(P_i)$ ва $(C_1, P_1 = D_k(C_1))$, $C, P_2 = E_k(C_2))$, $(C_3, P_3 = D_k(C_3))$,…, $(C_i, P_i = E_k(C_i)$ жуфтликлар маълум. Криптотаҳлилчининг вазифаси k – калитни топиш.

7) Калит ҳақида маълумотга эга бўлиш мақсадида танлаб олинган калитлар ёрдамида таҳлил қилиш.

Криптотаҳлилчига шифрматн ва шифрлаш алгоритми маълум. Криптотаҳлилчи бир нечта калитни танлаб олади ва алгоритм ёрдамида махфий калитга яқин бўлган калитни топади, яъни $(P_1, C_1 = E_{k1}(P))$, $(P_2, C_2 = E_{k2}(P))$, $(P_3, C_3 = E_{k3}(P))$,…, $(P_n, C_n = E_{kn}(P)$ маълум. Криптотаҳлилчининг вазифаси $k_1, k_2, k_3, \dots, k_n$ калитларнинг боғликликлари асосида шу шифрлаш алгоритми билан олинган ихтиёрий $C -$ шифрматнни очадиган $k -$ калитни топиш.

Юқоридаги хужужум турлари, умуман олганда криптотаҳлилаш усулларининг асосий мақсади шифрлаш калитига қаратилган бўлади. Сабаби ҳаммага маълумки симметрик алгоритмларда шифрлаш калити билан маълумотни дешифрлаш мумкин. Шунинг учун шифрлаш калитлари замонавий комъютерлар имкониятини ҳисобга олиб бардошли қилиб танланади.

*Замонавий криптотаҳлил усуллари ва ҳужум турлари:*Симметрик блокли шифрлаш алгоритмларининг бардошлилигини баҳолашда классик ҳужумлардан ташқари, алгоритмнинг ички тузилишига ва унинг аппарат воситаларидаги реализациясига йўналтирилган замонавий ҳужум турлари муҳим аҳамият касб этади.[65]

Дифференциал криптотаҳлил (Differential Cryptanalysis). Бу ҳужум тури очиқ матнлар орасидаги маълум бир фарқ (дифференциал)нинг шифрматнлар орасидаги фарққа таъсирини ўрганишга асосланади. Бунда криптотаҳлилчи алгоритмнинг ночизиқли қисми бўлган S-блоклар орқали маълум бир фарқнинг ўтиш эҳтимоллигини ҳисоблайди. S-блокларнинг "дифференциал бир хиллик" (Differential Uniformity) кўрсаткичи қанчалик паст бўлса, алгоритм ушбу ҳужумга шунчалик чидамли ҳисобланади.

Чизиқли криптотаҳлил (Linear Cryptanalysis). Мазкур усул очиқ матн, шифрматн ва калит битлари орасидаги чизиқли (математик) боғланишларни эҳтимоллик асосида қидиришга йўналтирилган. Бу ҳужум тури S-блокларнинг "чизиқсизлик даражаси" (Nonlinearity) билан бевосита боғлиқ бўлиб, S-блокларнинг чизиқсизлик даражаси юқори бўлиши алгоритмнинг ушбу ҳужумдан ҳимояланиш қобилиятини оширади.

Алгебраик ҳужумлар (Algebraic Attacks). Бунда шифрлаш жараёни кўпҳадли мантиқий тенгламалар тизими сифатида ифодаланади. Ҳужумнинг мақсади ушбу тенгламалар тизимини ечиш орқали махфий калитни тиклашдан иборат. S-блокларнинг "алгебраик иммунитети" ушбу ҳужумларга қаршиликни белгиловчи асосий мезондир.

Ён канал ҳужумлари (Side-Channel Attacks - SCA). Ушбу ҳужумлар алгоритмнинг математик заифлигига эмас, балки унинг техник қурилмада (масалан, микроконтроллерда) ишлаш жараёнидаги физик хусусиятларига асосланади:

Вақт бўйича ҳужум (Timing Attack): Шифрлаш амалиётининг турли калитлар билан ишлаш вақтини ўлчаш орқали калитни аниқлаш.

Қувват истеъмоли бўйича ҳужум (Power Analysis): Қурилманинг шифрлаш пайтида сарфлаётган электр энергиясини (SPA/DPA усуллари) таҳлил қилиш.[63]

Электромагнит нурланиш ҳужумлари: Қурилма ишлаётган пайтда чиқараётган электромагнит тўлқинларни масофадан туриб таҳлил қилиш.

Квант ҳужумлари (Quantum Attacks). Келажакда квант компьютерларининг пайдо бўлиши билан Гровер (Grover) алгоритми ёрдамида симметрик шифр калитларини танлаш тезлиги кескин ортади. Бу эса симметрик алгоритм калит узунлигини (масалан, 128 битдан 256 битгача) оширишни тақозо этади.

Келажакда квант компьютерларининг пайдо бўлиши ва уларнинг ҳисоблаш қувватлари ортиши ҳозирги замон криптографик стандартлари учун жиддий хавф туғдиради. Бу йўналишдаги ҳужумлар иккита асосий квант алгоритмига таянади:

Гровер (Grover) алгоритми ва симметрик шифрлаш: Гровер алгоритми ёрдамида симметрик шифр калитларини "қўпол куч" (brute-force) усули билан қидириш тезлиги квадрат илдиз даражасида тезлашади. Бу шуни англатадики, квант компьютери қаршисида 128 битли калитнинг бардошлилиги 64 битга, 256 битли калитники эса 128 битга тушиб қолади. Шу сабабли, замонавий талаблар асосида симметрик алгоритм калит узунлигини камида 256 битгача ошириш тақозо этилади.

Шор (Shor) алгоритми ва очиқ калитли тизимлар: Гарчи симметрик шифрлар квант ҳужумларига маълум даражада бардошли бўлса-да, Шор алгоритми кўпгина очиқ калитли криптотизимларни (масалан, RSA, ECC) тўлиқ бузиш имконини беради. Бу эса симметрик шифрлаш алгоритмларидаги калитларни алмашиш протоколларини ҳам қайта кўриб чиқишни талаб этади.

S-блокларнинг квант бардошлилиги. Квант ҳужумлари шароитида симметрик блокли шифрлаш алгоритмларининг асосий ночизиқли элементи бўлган S-блокларнинг (S-boxes) роли янада ортади. S-блокларнинг алгебраик мураккаблиги ва чизиқсизлик даражаси юқори бўлиши алгоритмнинг квант криптотаҳлилига қарши қўшимча ҳимоя қатламини яратади.[80]

Постквант даврига ўтиш. Ҳозирги кунда криптография соҳасида "Post-Quantum Cryptography" (Постквант криптографияси) йўналиши жадал ривожланмоқда. Бунда асосий эътибор квант компьютерлари ҳам ечишга қийналадиган математик муаммоларга (масалан, панжараларга асосланган криптография ёки кўп ўзгарувчили кўпҳадлар) қаратилган. Шу сабабли, яратилаётган автоматлаштирилган дастурий воситаларда S-блокларни таҳлил қилиш жараёнида уларнинг нафақат классик, балки квант криптотаҳлилига чидамлилик кўрсаткичларини ҳам ҳисобга олиш истиқболли ҳисобланади.

Юқоридаги ҳужум турларининг ривожланиши симметрик блокли шифрлаш алгоритмларининг асосий элементи бўлган S-блокларни лойиҳалашда уларнинг криптографик кўрсаткичларини

автоматлаштирилган дастурий воситалар ёрдамида комплекс таҳлил қилишни давр талабига айлантирмоқда.[64]

2.3. Симметрик шифрлаш алгоритми алмаштиришларини умумий криптографик талаблар бўйича баҳолаш

Симметрик шифрлаш алгоритмлари ҳар қандай криптографик алмаштиришларини $GF(2^n)$ фазони $X = (x_1, x_2, \dots, x_n)$, бошқа $GF(2^m)$ фазога $Y = (y_1, y_2, \dots, y_n)$ акслантириш сифатида қараб, ушбу акслантиришни буль функциялар орқали қуйидагича ифодалаш мумкин.

$$Y = \varphi(X): GF(2^n) \to GF(2^m), X = (x_1, x_2, \dots, x_n), Y = (y_1, y_2, \dots, y_n)$$

Акслантириш эса $\varphi(X) = \{f_1(X), f_1(X), \dots, f_m(X)\}$ – вектор буль функциялар (компоненталар) кўринишида тасвирланади. Бу ерда $f_i, x_i, y_i \in GF(2)$ $(f_i, x_i, y_i = \{0,1\}$. Демак, блокли симметрик шифрлаш алгоритмидаги бирор криптографик алмаштиришни баҳолаш жараёнида унга математик модел бўлган, берилган буль функция хоссаларини ўрганиш етарли ҳисобланади.

Мазкур келтирилган тушунчалардан маълумки, блокли симметрик шифрлаш алгоритми алмаштиришларининг юқорида келтирилган барча хоссалари ва сонли характеристикалари ушбу шифрлаш алгоритмининг криптобардошлилигига ўз таъсирини кўрсатади. Шунга кўра, бирор блокли симметрик шифрлаш алгоритми (ўрнига қўйиш) алмаштиришига нисбатан юқоридаги фикрларни умумлаштирган ҳолда ишлаб чиқилган умумий криптографик талаблар қуйида келтирилган :

1. $Y = \varphi(X) = \{f_1(X), f_1(X), \dots, f_m(X)\}: GF(2^n) \rightarrow GF(2^m)$ акслантиришни ташкил этувчи $f_i(X)$ бул функцияларининг баланслашган бўлишлиги;

2. $f_i(X)$ – буль функцияларнинг алгебраик чизиқсизлик даражасини $\deg(f_i(X))$ – юқори бўлишлиги;

3. $f_i(X)$– буль функцияларнинг юқори корреляцион иммунитетлик даражаларига эга бўлишлиги;

4. $f_i(X)$ – буль функцияларнинг юқори тартибли қатъий лавин самарадорлик (SAC) ва тарқалиш тамойиллари (PC) кўрсаткичларига эга бўлишлиги.

5. $f_i(X)$ – буль функцияларнинг юқори чизиқсизлик қийматларига $N(f_i(X))$ эга бўлишлиги.

6. $\varphi(X)$ – акслантириш учун $N(\varphi(X))$ – қийматнинг катта ва $L(\varphi(X))$қийматнинг кичик бўлишлиги;

7. $\varphi(X)$ – акслантириш учун $AI(\varphi(X))$ – қийматнинг катта бўлишлиги;

8. $\varphi(X)$ – акслантириш учун BIC – қийматнинг нолга яқин бўлишлиги.

Криптография амалиёти шуни кўрсатадики, мазкур келтирилган барча талабларни қаноатлантирувчи ягона буль функция ёки акслантиришлар мавжуд эмас. Бунинг сабаби, айрим талабларнинг ўзаро зидлиги (масалан: чизиқсизлик ва корреляцион иммунитетлик тушунчалари ўзаро зид) ҳисобланади. Шу боис, шифрлаш алгоритмлари таркибида у ёки бу талабни қаноатлантирувчи функцияларнинг комбинациясидан фойдаланиш мақсадга мувофиқ бўлади. Таъкидлаш лозимки, блокли симметрик шифрлаш

алгоритмлари криптобардошли-лигини таъминлашда мазкур келтирилган талаблар зарурий, бироқ етарли ҳисобланмайди. Шунингдек, турли ёндашувдаги криптотаҳлил усулларининг вужудга келиши ушбу криптографик талаблар сонини ошишига ҳам олиб келади.[16]

Умумий ҳолда, янги таклиф этилган ёки мавжуд стандарт блокли симметрик шифрлаш алгоритми акслантириш-ларини криптографик талаблар бўйича баҳолаш жараёни қуйидаги “Баҳолаш натижалари” 2.3-жадвалини тўлдириш ва у асосида алгоритм бардошлилиги юзасидан тегишли хулоса чиқариш босқичларини ўз ичига олади.

2.3-жадвал

Баҳолаш натижалари

№	Бажарилувчи иш	Иш натижаси	Иш хулосаси
1.	Акслантиришларнинг кириш ва чиқиш битларига мос чинлик жадвалларини тузиш	Чинлик жадвалини амалий қуриш мумкин	Кейинги босқичга ўтиш мумкин
		Чинлик жадвалини амалий қуриб бўлмайди	Текширилаётган акслантиришни чинлик жадвали асосида баҳолаб бўлмайди
2.	Акслантиришларнинг мос буль функция компоненталари учун АНФлар қуриш ва	$\deg(f_i(X))$– қиймати максимал (ёки унга яқин)	Кейинги босқичга ўтиш мумкин

	уларнинг deg $(f_i(X))$ параметр қийматларини Аниқлаш	deg (f_i)=1	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш каби фойдаланиб бўлмайди
3.	Акслантиришлар (буль компоненталари) учун регулярлик (балансланганлик) хоссасини текшириш	Регуляр (балансланган)	Кейинги босқичга ўтиш мумкин
		Регуляр (балансланган) эмас	Текширилаётган акслантириш заифликка эга бўлиб, ундан шифрлаш алгоритми таркибида фойдаланиш мақсадга мувофиқ эмас
4.	Акслантиришлар мос буль функция компоненталари учун $CI(f_i)$– параметр қийматини аниқлаш	$CI(f_i)$– – қиймати максимал (ёки унга яқин)	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш сифатида фойдаланиб бўлмайди
		$CI(f_i)$=0	Кейинги босқичга ўтиш мумкин
5.	Акслантиришлар (буль	$N(\varphi(x))(N(f_i))$– қиймати	Кейинги босқичга ўтиш мумкин

	компоненталари) учун $N(\varphi(x))(N(f_i))$– параметр қийматини аниқлаш	максимал (ёки унга яқин)	
		$N\left(\varphi(x)\right) = 0$ $(N(f_i))=0$	Текширилаётган акслантиришдан шифрлаш алгоритми таркибида чизиқсиз акслантириш сифатида фойдаланиб бўлмайди
6.	Акслантиришлар мос буль функция компоненталари учун $SAC(f_i)$ – параметр қийматини аниқлаш	$SAC(f_i)$	Кейинги босқичга ўтиш мумкин
7.	Акслантиришлар учун $AI(\varphi(x))$ – параметр қийматини аниқлаш	$AI(\varphi(x))$ қиймати максимал (ёки унга яқин)	Кейинги босқичга ўтиш мумкин
		$AI\left(\varphi(x)\right) = 1$	Текширилаётган акслантиришдан шифрлаш алгоритмини алгебраик криптотаҳлил усулига бардошлиликни таъминловчи акслантириш сифатида фойдаланиб бўлмайди

8.	Якуний хулоса	Юқорида олинган криптографик талаблар натижалари асосида алгоритм крипто-бардошлиги юзасидан хулоса чиқариш – барча кўрсаткичларни умумлаштирган ҳолда амалга оширилади. Агар барча криптографик талаблар алгоритмнинг мос равишда бирор акслантириши орқали максимал (ёки унга яқин) бажарилса, у ҳолда “алгоритм криптобардошли бўлиши мумкин” деб, аксинча, айрим талабларни қаноатлантирувчи бирорта ҳам акслантириш мавжуд бўлмаса “алгоритм заифликка эга (криптобардошсиз) бўлиши мумкин” деб хулоса чиқариш мақсадга мувофиқ.

Таъкидлаш лозимки, криптографик талабларга мос параметр қийматларини амалий ҳисоблаш имконияти блокли симметрик шифрлаш алгоритмлари учун муҳим аҳамият касб этади. Агарда, акслантиришларни умумий криптографик талабларга текширишнинг амалий имконияти мавжуд бўлмаса, у ҳолда шифрлаш алгоритми акслантиришининг бардошлилиги ёки бардошсизлиги юзасидан хулоса чиқариш нотўғри ҳисобланади.[46]

2.3.1.Дифференциал бир хиллик

Замонавий симметрик блокли шифрлаш алгоритмларининг хавфсизлиги асосан иккита фундаментал принципга— **диффузия** (тарқалиш)ва **конфузия** (алмаштириш) хусусиятларига таянади. Алгоритмнинг чизиқли бўлмаган алмаштириш қатлами, яъни **S-блоклар** (Substitution-boxes), конфузия

эффектини таъминловчи ягона ва энг муҳим компонент ҳисобланади.S-блокларнинг асосий вазифаси — кириш ва чиқиш маълумотлари ўртасидаги боғлиқликни математик жиҳатдан мураккаблаштириш орқали алгоритмнинг чизиқли ҳужумларга (Linear Cryptanalysis) ва дифференциал ҳужумларга (Differential Cryptanalysis) чидамлилигини таъминлашдир. S-блокларнинг криптографик сифатини баҳолашда уларнинг **чизиқли бўлмаган хусусиятлари** (Non-linear properties) биринчи даражали аҳамиятга эга. Агар S-блок чизиқли ёки чизиқлиликка яқин бўлса, тайёргарлик кўрган тажовузкор алгебраик тенгламалар тизимини тузиш орқали махфий калитни осонгина аниқлаши мумкин. Шу сабабли, замонавий криптографик талабларга кўра, S-блоклар юқори даражадаги чизиқли бўлмаганлик (Nonlinearity) ва минимал **дифференциал бир хиллик** (Differential Uniformity) кўрсаткичларига эга бўлиши шарт.[47]

Қуйида S-блокларнинг дифференциал ҳужумларга бардошлилик даражасини белгиловчи дифференциал бир хиллик кўрсаткичи ва унинг таҳлилини батафсил кўриб чиқамиз.

Симметрик шифрлаш алгоритмларининг S-блоклари дифференциал криптоанализ ҳужумларига бардошли бўлиши учун уларнинг **дифференциал бир хиллик** (Differential Uniformity) кўрсаткичи имкон қадар паст бўлиши талаб этилади. Ушбу кўрсаткич киришдаги фарқларнинг чиқишдаги фарқларга таъсир қилиш эҳтимоллигини миқдорий жиҳатдан ифодалайди.

Математик нуқтаи назардан, $F: F_2 \rightarrow F_{2^m}$ кўринишидаги n-битли кириш ва m-битли чиқишга эга бўлган S-блок (чизиқли

бўлмаган функция) учун ихтиёрий $a \in F_{2^n}\{0\}$ (кириш фарқи) ва $b \in F_{2^m}$ (чиқиш фарқи) берилган бўлсин. Ушбу қийматлар учун қуйидаги дифференциал тенгламани кўриб чиқамиз:

$$F(x \otimes a) \oplus F(x) = b$$

Бу ерда $\otimes$ амали $GF(2^n)$ майдонидаги қўшиш (XOR) амалини англатади хамда a ва b **дифференциал ўтиши** деб аталади. Агар $N_F(a, b)$ қиймати катта бўлса, демак, киришдаги a фарқи чиқишда b фарқини ҳосил қилиш эҳтимоллиги юқори бўлади . Юқоридаги тенгламанинг x бўйича ечимлар сони билан белгиланади:

$$N_F(a + b) = |\{x \epsilon F_{2^n} : F(x \otimes a) \otimes F(x) = b\}|$$

Функциянинг **дифференциал бир хиллиги** ($\boldsymbol{\delta_F}$) деб, барча мумкин бўлган $a \neq 0$ ва b жуфтликлари учун ушбу ечимлар сонининг энг катта (максимал) қийматига айтилади:

$$\boldsymbol{\delta_F} = \max_{a \neq 0, b \in F_2} N_F(a, b)$$

Криптографик баҳолаш мезонларига кўра, ($\boldsymbol{\delta_F}$) қиймати қанчалик кичик бўлса, S-блок дифференциал ҳужумларга шунчалик чидамли ҳисобланади.

Агар $\boldsymbol{\delta_F} = \mathbf{2}$ бўлса, бундай функциялар APN (Almost Perfect Nonlinear) функциялар деб аталади ва улар энг юқори чидамлилик даражасига эга.

Агар $\boldsymbol{\delta_F} = \mathbf{4}$ бўлса, бу кўрсаткич замонавий стандартлар (масалан, AES) учун етарлича хавфсиз ҳисобланади.

Дифференциал бир хилликнинг паст қиймати тажовузкор учун шифрланган матнлар орасидаги статистик боғлиқликни аниқлашни мураккаблаштиради ва муваффақиятли ҳужум эҳтимоллигини минималлаштиради.[35]

Эҳтимоллик хусусияти-S-блок орқали маълум бир дифференциал ўтишнинг амалга ошиш эҳтимоллиги $P_F(a,b) = N_F(a,b)/2^n$ формуласи билан аниқланади. Дифференциал бир хиллик ($\boldsymbol{\delta_F}$) эса энг катта ўтиш эҳтимоллигини чегаралайди:

$$P_{max} = \frac{\delta_F}{2^n}$$

Масалан, AES алгоритмида $\boldsymbol{\delta_F = 4}$ ва n=8 бўлгани учун максимал эҳтимоллик 4/256=0.0156 ни ташкил этади. Бу кўрсаткич қанчалик кичик бўлса, тажовузкор учун шифрлашнинг кўп раундли занжирларида "дифференциал йўл" (differential characteristic) қуриш шунчалик мураккаб бўлади.

Ечимлар сонининг жуфтлиги: $\boldsymbol{F_{2^n}}$ майдонидаги ҳар қандай функция учун, агар x ушбу тенгламанинг ечими бўлса, у ҳолда

$x \otimes a$ ҳам албатта унинг ечими бўлади. Шу сабабли $N_F(a,b)$ қиймати доимо **жуфт сон** (0, 2, 4, ...) бўлиши шарт. Бу хусусият характеристикаси 2 га тенг бўлган майдонлар учун хосдир.

Идеал кўрсаткич (APN):

Жуфт сонли майдонларда (F_{2^n}) энг кичик мумкин бўлган максимал ечимлар сони $\boldsymbol{\delta_F = 2}$ га тенг. Бундай кўрсаткичга эга функциялар **Almost Perfect Nonlinear (APN)** деб аталади ва улар назарий жиҳатдан дифференциал криптоанализдан энг мукаммал ҳимояни таъминлайди.

2.3.2. Дифференциал тарқалиш жадвали (DDT) ва натижалар таҳлили.

S-блокнинг дифференциал хусусиятларини тизимли равишда ўрганиш ва барча мумкин бўлган кириш/чиқиш фарқларини таҳлил қилиш учун **Дифференциал тарқалиш жадвали** (Differential Distribution Table — DDT) қурилади. Ушбу жадвал S-блокнинг криптографик мустаҳкамлигини миқдорий баҳолаш имконини беради.

Қуйида мисол тариқасида 4-битли S-блок учун ҳисобланган DDT жадвали келтирилган.

2.3.2 -жадвал

$\triangle x \backslash \triangle y$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Жадвал изоҳи: Жадвалнинг a-қатори ва b-устунидаги қиймат $N_F(a, b)$ ечимлар сонини ифодалайди.

Жадвал таҳлили шуни кўрсатадики, биринчи қатор ва устундан ташқари (бу ерда $a \neq 0$) энг катта қиймат **4** га тенг. Демак, ушбу S-

блок учун **дифференциал бир хиллик кўрсаткичи $\boldsymbol{\delta_F = 4}$** ни ташкил этади.[36]

S-блокларнинг чизиқли бўлмаганлик (Nonlinearity) кўрсаткичи.

S-блокларнинг чизиқли ҳужумларга (Linear Cryptanalysis) чидамлилиги уларнинг **чизиқли бўлмаганлик** (L_F ёки $NL(F)$ параметри билан белгиланади. Ушбу кўрсаткич F функциясининг барча мумкин бўлган чизиқли функциялар тўпламидан қанчалик "узоқда" жойлашганлигини ўлчайди.

Математик жиҳатдан, n-битли F функцияси учун чизиқли бўлмаганлик кўрсаткичи **Уолш-Адамар алмашмаси** (Walsh-Hadamard Transform) ёрдамида қуйидагича аниқланади:

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n, b \in F_2^n, a \neq 0} |W_F(a,b)|$$

Бу ерда $W_F(a,b)$ — функциянинг Уолш-Адамар коэффициенти бўлиб, у кириш ва чиқиш битларининг чизиқли комбинациялари ўртасидаги боғлиқликни ифодалайди.

1. *Ҳужумдан ҳимоя*: $NL(F)$ қиймати қанчалик юқори бўлса, тажовузкор учун шифрлаш жараёнини чизиқли тенгламалар ёрдамида аппроксимация қилиш (яқинлаштириш) шунчалик мураккаб бўлади.
2. *Идеал кўрсаткич (Bent функциялар)*:n -битли функциялар учун максимал мумкин бўлган чизиқли бўлмаганлик қиймати $2^{n-1} - 2^{\frac{n}{2}-1}$ га тенг. Бундай функциялар Bent функциялар деб аталади.

3. *Амалий талаблар*: Масалан, 8-битли AES S-бохи учун NL(F) =112 га тенг. Бу жуда юқори кўрсаткич ҳисобланиб, чизиқли ҳужум эҳтимоллигини 2^{-128} дан паст даражага туширади.

Чизиқли аппроксимация жадвали (LAT)

S-блокнинг чизиқли хусусиятларини таҳлил қилиш учун **Чизиқли аппроксимация жадвали** (Linear Approximation Table — LAT) қурилади. LAT жадвалидаги ҳар бир элемент кириш битларининг суммаси ва чиқиш битларининг суммаси ўртасидаги мосликни кўрсатади.

Чизиқли бўлмаганлик кўрсаткичининг криптографик аҳамияти:

2.3.3-жадвал

$\alpha\backslash\beta$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	+8	0	0	0	0	0	0	0
1	0	0	-2	+2	0	0	-2	-2
2	0	-2	0	-2	+4	-2	0	+2

Изоҳ: Жадвалдаги қийматлар 8 дан (яъни 2^{n-1} дан) қанчалик кўп фарқ қилса, S-блок шунчалик кучли чизиқли бўлмаганликка эга бўлади.

Хулосавий баҳолаш:Шундай қилиб, симметрик шифрлаш алгоритмининг алмаштиришларини баҳолашда **дифференциал бир хиллик (δ_F)** ва **чизиқли бўлмаганлик (NL)** кўрсаткичлари бир-бирини тўлдиради. Оптимал лойиҳаланган S-блок

учун $(\boldsymbol{\delta_F})$ минимал, NL эса максимал қийматга эга бўлиши шарт. Бу икки шартнинг бажарилиши алгоритмнинг замонавий статистик криптоанализ усулларига нисбатан бардошлилигини кафолатлайди.[69]

Боб бўйича хулоса

Хулоса қилиб айтганда, ушбу бобда симметрик блокли шифрлаш алгоритмларининг криптобардошлилигини баҳолашнинг назарий ва методологик асослари тизимли равишда тадқиқ этилди. Олиб борилган изланишлар асосида қуйидаги якуний фикрларни шакллантириш мумкин:

1.Криптобардошлилик мезонлари: Симметрик блокли шифрлаш алгоритмларини замонавий криптографик талаблар бўйича баҳолаш усуллари таҳлил қилинди. Алгоритм хавфсизлиги нафақат калит узунлигига, балки алмаштириш блокларининг (S-box) математик мураккаблигига — хусусан, уларнинг дифференциал бир хиллиги (δ_F) ва чизиқли бўлмаганлик (NL) кўрсаткичларига бевосита боғлиқ эканлиги асослаб берилди.

2.Криптотаҳлил усуллари ва ҳужум турлари: Криптографик алгоритмларга нисбатан қўлланиладиган ҳужум турлари классификацияси кўриб чиқилди. Таҳлил жараёнида шифрматн асосидаги, очиқ матн ва шифрматн жуфтлиги ҳамда танлаб олинган очиқ матн асосидаги ҳужум моделларининг алгоритм ички структурасига таъсири ўрганилди.

3.Баҳолаш методикаси ва S-блок таҳлили: Шифрлаш алгоритмларини таҳлил қилишда Дифференциал тарқалиш жадвали

(DDT) ва Чизиқли аппроксимация жадвали (LAT) дан фойдаланишнинг аҳамияти ёритилди. Тадқиқотлар шуни кўрсатдики, S-блокларнинг дифференциал бир хиллик кўрсаткичининг пастлиги ($\delta_F \leq 0$) ва чизиқли бўлмаганлик даражасининг юқорилиги алгоритмнинг дифференциал ва чизиқли криптотаҳлилга чидамлилигини таъминловчи асосий омиллардир.

4.Амалий аҳамияти: Ўрганилган баҳолаш усуллари ва математик моделлар келгуси бобда ишлаб чиқиладиган автоматлаштирилган дастурий воситанинг алгоритмик асоси бўлиб хизмат қилади. Бу эса миллий шифрлаш стандартларини криптографик талабларга мувофиқлигини тезкор ва аниқ текшириш имконини яратади.[46,47]

II БОБ. СИММЕТРИК БЛОКЛИ ШИФРЛАШ АЛГОРИТМЛАРИНИНГ S ЖАДВАЛЛАРИНИ КРИПТОТАҲЛИЛОВЧИ АВТОМАТЛАШГАН ДАСТУРИЙ ВОСИТАЛАРИНИ ИШЛАБ ЧИҚИШ

3.1. Криптографик алгоиртмларни криптоанализ қилувчи автоматлашган дастурий воситани ишлаб чиқиш

Криптотаҳлил усуллари таҳлили шуни кўрсатдики, шифрлаш алгоритмларида асосий акслантириш чизиқсиз алмаштириш, яъни, S-блок акслантириши ҳисобланади. Шу сабабли, Borland Delphi дастурлаш муҳитида S-блок акслантириш жадвалини умумий криптографик талабларга текширувчи автоматлаштирилган дастурий таъминот яратилди.

Умумий криптографик талабларга баланслашганлик, регулярлик, чизиқсизлик, алгебраик иммунитет, корреляцион иммунитет, қатъий лавин самарадорлиги каби параметрлар киради.

Баланслашганлик параметрини аниқлаш дастурий код ёрдамида аниқланди:

```
sum:=0;
 for i := 0 to Length(s_блок)-1 do
 begin
  sum:=sum xor s_блок[i];
 end;
 if sum=0 then Memo1.Lines.Add('Balance=Ha') else Memo1.Lines.Add('Balance=Yo’q);
```

Регулярлик шартини аниқлаш коди қуйидагича:

```
if regulyarlik then Memo1.Lines.Add('Regulyar=Ha') else
```

```
Memo1.Lines.Add('Regulyar=Yo`q')
```

Бу ерда регулярлик функцияси s_блок массивининг регулярлик шартини қаноатлантиришини текширади, ва натижани true ёки false қиймат сифатида қайтаради.

```
function regulyarlik():boolean;
var i,j,l:integer;b:boolean;
begin
b:=true;
l:=trunc(sqrt(Length(s_блок)));
 for i:=0 to l-2 do
 for j:=i+1 to l-1 do
 begin
 if s_блок[i]=s_блок[j] then b:=false;
 end;
 regulyarlik:=b;
end;
```

Алгебраик иммунитет тушунчаси акслантиришни ифодаловчи буль функциялар учун шакллантирилган буль тенгламалар системасининг минимал алгебраик даражасини англатади. Мазкур параметрни акслантиришни ифодаловчи тенгламаларни шакллантиргандан сўнг аниқлаш мумкин. Киритилган алмаштириш жадвалига нисбатан тенгламалар системасини шакллантирувчи дастурий код тузилди. Дастур матни иловада келтирилади. [35,75]

Чизиқсизлик параметрини аниқлаш учун қуйидаги дастур коди ёзилди:

```
for i:=0 to n-1 do
```

```
begin
 ua[i]:=ualsh_adamar(s_блок,i);
end;
chiziqsizlik:=trunc(ikki_daraja(S_ulcham-1)-0.5*max(ua));
Memo1.Lines.Add('N(f1)='+ inttostr(chiziqsizlik));
```

Бу ерда ualsh_adamar(s_блок,i) функцияси i вектор учун Уалш-Адамар алмаштириши қийматини қайтаради. Мазкур функциянинг матни қуйидагича:

```
function ualsh_adamar(a:array of integer;b:integer):integer;
var l,i,j,s,u,h:integer;
begin
  l:=Length(a);
  j:=trunc(sqrt(l));
  s:=0;
  u:=0;
  h:=0;
  for i:=0 to l-1 do
  begin
  h:= skalyar(i,b,j);
   s:=a[i] xor h;
   if s mod 2 =0 then u:=u+1
   else u:=u-1;
  end;
  ualsh_adamar:=u;
end;
```

скаляр (i,b,j) функция j разрядли i ва b векторларининг скаляр кўпайтмасини ҳисоблайди:

```
function skalyar (a:integer;b:integer;p:integer):integer;
var s,i,c:integer;
begin
s:=0;
c:=a and b;
  for i:=1 to p do
  begin
    s:=s+(c mod 2);
    c:=c shr 1;
  end;
skalyar :=s;
end;
```

Чизиқсизликни ҳисоблашда фойдаланилган max(u:array of integer) функцияси берилган Уалш-Адамар алмаштириш қийматлари массиви элементларининг максимал қийматини қайтаради.

```
function max(u:array of integer):integer;
var m,l,i:integer;
begin
   l:=Length(u);
   m:=abs(u[0]);
   for i:=1 to l-1 do
   if abs(u[i])>m then m:=abs(u[i]);
   max:=m;
end;
```

Корреляцион иммунитет параметрини ҳисоблаш процедураси кўриниши қуйидагича:

```
SetLength(ci_bool1,n);
 for k:=0 to S_ulcham-1 do
begin
 ci_bool1[k]:=false;
end;
SetLength(xeming_bitlar,n);
 for i:=0 to n-1 do
 begin
 xeming_bitlar[i]:=xeming(i,S_ulcham);
 end;
 //ShowMessage('x[n]='+inttostr(xeming_bitlar[n-1]));
 for i:=1 to n-1 do
  begin
  ua[i]:=ualsh_adamar(s_блок,i);
  k:=summa(ua);
  if ua[i]=0 then
  begin
    ci_bool1[i]:=true;
  end else ci_bool1[i]:=false;
  end;
 SetLength(i_bool2,S_ulcham+1);
 for i:=0 to S_ulcham do
 begin k:=0;
  for j:=0 to n-1 do
```

```
 if (xeming_bitlar[j]=i)then k:=k+1;
 i_bool2[i]:=k;
end;
for i:=0 to S_ulcham do
begin
 k:=0;
 for j:=0 to n-2 do
  if ((xeming_bitlar[j]=i)and (ci_bool1[j]=true)) then k:=k+1;
 if (k=i_bool2[i]) then CI:=i;
end;
Memo1.Lines.Add('CI(S)='+IntToStr(CI));
```

xeming(i,S_ulcham) функция S_улчам разрядли i сонининг Хеминг оғирлигини ҳисоблайди.

xeming_bitlar[i] эса i сонининг Хеминг оғирлиги қийматини сақлайди.

ua[i] - i сонига нисбатан Уалш-Адамар алмаштириш қийматини сақлайди.

summa(ua) - Уалш-Адамар алмаштириш қийматлари массивининг 2 модуль бўйича йиғиндисини ҳисоблайди.

Қатъий лавин самарадорлик жаражасини аниқлаш процедураси кўриниши қуйидагича кўринишга эга:

```
procedure TForm1.Button6Click(Sender: TObject);
begin
   SetLength(beta,S_ulcham);
   for i:=0 to S_ulcham-1 do
   beta[i]:=ikki_daraja(i);
```

```
SAC:=0;
for i:=1 to n-1 do
begin
 for h1:=0 to n do
 begin
  k:=0;
  h2:=0;
  if (h1 and i=i) then
  begin
    k:=k+1;
   if balanslashgan(s_блок,h1,S_ulcham)=true then h2:=h2+1;
  end;
 end;
 if (k=h2)and (k<>0) then SAC:=xeming_bitlar[i];
end;
beta:=nil;
s_блок:=nil;
s_b:=nil;
Memo1.Lines.Add('SAC(S)='+inttostr(SAC));
end;
```

Бу ерда фойдаланилган balanslashgan(s_блок,h1,S_ulcham) буль функиянинг баланслашган ёки баланслашмаганлигини аниқлайди:

```
function balanslashgan(a:array of integer; b:integer;c:integer):bool;
var i,s:integer;
begin
 s:=0;
```

```
  for i:=0 to c-1 do
   s:=s+(a[b] xor a[b xor beta[i]]);
  if s=0 then balanslashgan:=true else balanslashgan:=false;
end;
```

3.1.1. Дастурий воситанинг вазифалари ва архитектураси.

Ишлаб чиқилган автоматлаштирилган дастурий воситанинг бош мақсади — симметрик блокли шифрлаш алгоритмларининг асосий элементи ҳисобланган S-блокларнинг (алмаштириш жадвалларининг) криптографик бардошлилик талабларига мувофиқлигини тезкор ва аниқ баҳолашдан иборат. Дастурий таъминот криптоаналитик тадқиқотлар жараёнида инсон омилини камайтириш ва мураккаб математик ҳисоблашларни автоматлаштириш имконини беради.[77]

Дастурий воситанинг асосий вазифалари:Дастурий таъминот фойдаланувчига қуйидаги амалий имкониятларни тақдим этади:

Маълумотларни киритиш ва бошқариш: S-блок қийматларини турли форматларда (HEX, DEC) киритиш, уларни таҳрирлаш ва таҳлил учун тайёрлаш.

Математик хоссаларни ҳисоблаш: S-блокнинг Бул функциялари асосида унинг фундаментал криптографик кўрсаткичларини аниқлаш.

Криптобардошлилик таҳлили: Олинган натижаларни назарий жиҳатдан хавфсиз деб ҳисобланган қийматлар билан солиштириш.

Хулоса чиқариш: Таҳлил натижалари асосида конкрет S-блокнинг маълум бир шифрлаш алгоритмида (масалан, енгил вазнли шифрларда ёки стандарт тизимларда) қўлланилиши мумкинлиги ҳақида якуний хулоса бериш.

Дастурий воситанинг архитектураси:Дастур модулли архитектура тамойили асосида қурилган бўлиб, у қуйидаги таркибий қисмлардан иборат:

Интерфейс модули (User Interface Layer): Фойдаланувчи билан мулоқотни таъминлайди. Бу ерда S-блок ўлчамлари (4x4, 5x5, 8x8 ва ҳ.к.) танланади ва жадвал кўринишидаги маълумотлар киритилади.

Ҳисоблаш ядроси (Computational Engine): Дастурнинг энг муҳим қисми бўлиб, унда Уолш-Адамар алмаштириши, Хеминг масофасини ўлчаш ва Бул функцияларининг Алгебраик нормал шаклини (ANF) қуриш алгоритмлари жойлашган.

Таҳлил блоки (Analytical Block): Ушбу блок ҳисоблаш ядросидан олинган сонли қийматларни қуйидаги тўртта асосий мезон бўйича гуруҳлайди ва баҳолайди:

Баланслашганлик ва регулярлик: Чиқиш битларининг эҳтимоллик тақсимоти текислигини текшириш.

Чизиқсизлик даражаси (Nonlinearity): Функсиянинг чизиқли ҳужумларга (Linear Cryptanalysis) бардошлилик даражасини белгилаш.

Алгебраик ва корреляцион иммунитет: S-блокнинг алгебраик тенгламалар ёрдамида тасвирланиш мураккаблигини ва кириш-чиқиш битлари орасидаги статистик боғлиқлик йўқлигини аниқлаш.

Қатъий лавин самарадорлиги (SAC): Киришдаги бит ўзгаришининг чиқишга таъсир қилиш динамикасини (камида 50%) баҳолаш.

Ҳисобот бериш модули (Reporting Module): Таҳлил натижаларини визуал шаклда (матнли Memo майдонида ёки график кўринишда) фойдаланувчига тақдим этади.

Дастурнинг бундай кўп босқичли архитектураси унинг универсаллигини таъминлайди ва келажакда янги криптографик мезонлар (масалан, квант чидамлилиги кўрсаткичлари) билан кенгайтириш имконини беради.[15]

3.1.2. Алгоритмик реализация ва дастурий код таҳлили.

Дастурий воситанинг ишлаш жараёнида S-блокларнинг криптографик кўрсаткичларини ҳисоблаш учун махсус алгоритмлар ва оптимизаллаштирилган код тузилмаларидан фойдаланилган. Қуйида ҳар бир кўрсаткичнинг ҳисобланиш механизми ва унинг дастурий реализацияси батафсил таҳлил қилинади.

1. Баланслашганлик шартини текшириш алгоритми

S-блокнинг баланслашганлик хусусияти унинг чиқиш битлари орасида "0" ва "1" қийматларининг тенг тақсимланишини англатади. Бу статистик криптотаҳлил ҳужумларига қарши бирламчи ҳимоя ҳисобланади.

Дастурда бу жараён S-блокнинг барча чиқиш қийматларини бинар XOR (истисноли ЁКИ) амали орқали йиғиш асосида қурилган. Агар барча қийматларнинг XOR йиғиндиси нолга тенг бўлса, демак, жадвалдаги барча мумкин бўлган чиқиш қийматлари бир хил такрорланган ва тизим балансланган ҳисобланади.

Дастурий код таҳлили:

```
sum := 0;
for i := 0 to Length(s_блок) - 1 do
begin
    sum := sum xor s_блок[i]; // Ҳар бир элементни XOR йиғиндига қўшиш
```

```
end;
    if sum = 0 then
        Memo1.Lines.Add('Balance = Ha')
    else
        Memo1.Lines.Add('Balance = Yo’q');
```

Ушбу алгоритмнинг афзаллиги шундаки, у O(n) мураккабликда ишлайди ва катта ўлчамдаги (масалан, 8x8) S-блоклар учун ҳам жуда тезкор натижа беради.

2. Қатъий лавин самарадорлигини (SAC) баҳолаш механизми

Қатъий лавин самарадорлиги (Strict Avalanche Criterion) — бу шифрлаш алгоритмининг мураккаблигини белгиловчи муҳим мезондир. Унга кўра, кириш векторидаги исталган 1 битнинг ўзгариши чиқиш векторидаги битларнинг ўртача 50 фоизи ўзгаришига сабаб бўлиши керак.[33]

Дастурда буни ҳисоблаш учун иккита асосий элементдан фойдаланилган:

- xeming(i, S_ulcham) функцияси: Берилган соннинг бинар кўринишидаги "1"лар сонини (Хеминг оғирлигини) ҳисоблайди.
- beta массиви: Киришдаги ҳар бир позициядаги битнинг ўзгаришини $(2^0, 2^1, 2^2 \dots)$ симуляция қилувчи ниқоб (mask) вазифасини бажаради.

Дастурий реализация деталлари:

```
procedure TForm1.Button6Click(Sender: TObject);
begin
    SetLength(beta, S_ulcham);
    for i := 0 to S_ulcham - 1 do
```

```
        beta[i] := ikki_daraja(i);
        SAC := 0;
end;
        { Цикл давомида ҳар бир кириш вектори X учун S(X) ва S(X
        xor beta[i]) қийматлари орасидаги Хеминг масофаси ҳисобланади.
        Олинган натижа 0.5 эҳтимолликка қанчалик яқинлиги
        текширилади. }
```

Бунда дастур ҳар бир чиқиш битининг мустақиллигини ва ўзгариш эҳтимоллигини матрица кўринишида шакллантириб, якуний натижани фойдаланувчига тақдим этади.

3. Уолш-Адамар алмаштириши ва чизиқсизлик даражасини аниқлаш

Чизиқли криптотаҳлилга (Linear Cryptanalysis) қарши бардошлиликни таъминлаш учун S-блок иложи борича "чизиқсиз" бўлиши керак. Бу кўрсаткични ҳисоблаш учун дастурда Уолш-Адамар алмаштириши (Walsh-Hadamard Transform - WHT) алгоритми реализация қилинган.[12,27]

Ҳисоблаш босқичлари:

S-блокнинг Бул функциялари учун қийматлар жадвали шакллантирилади.

Ҳар бир функция учун WHT коэффитсиентлари ҳисобланади. Дастурда ua[i] массиви айнан шу коэффитсиентларни сақлайди.

Коэффитсиентларнинг максимал қиймати асосида Чизиқсизлик (Nonlinearity) индекси топилади:

$$NL = 2^{n-1} - \frac{1}{2} max\,|WHT(u)|$$

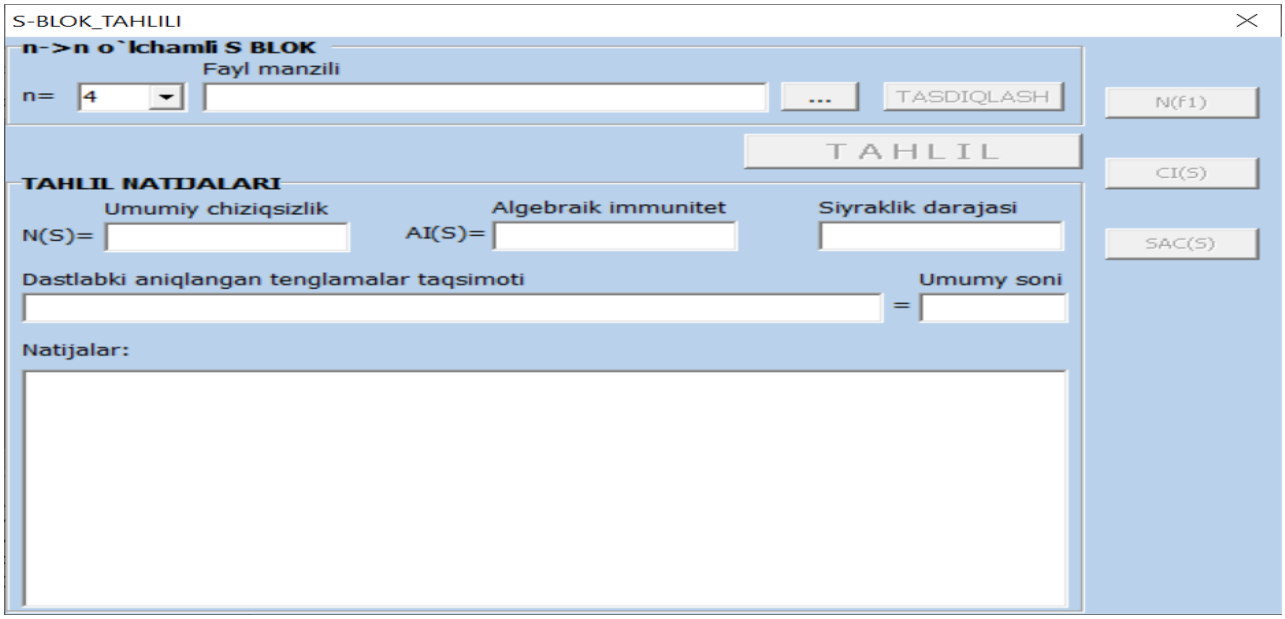
Шунингдек, дастур Корреляцион иммунитет (Correlation Immunity - CI) даражасини ҳам ҳисоблайди. Агар Уолш коэффитсиентлари маълум бир Хеминг оғирлигидаги векторлар учун нолга тенг бўлса, функция маълум тартибдаги CI га эга деб хулоса қилинади.

Натижаларни таҳлил қилиш блоки:

Дастурда Memo1 компоненти орқали чиқариладиган маълумотлар фойдаланувчига нафақат сонли қийматларни, балки жадвалнинг криптографик "сифати" ҳақидаги тавсияларни ҳам беради. Масалан, NL қиймати AES учун 112 га тенг бўлса, дастур уни "юқори бардошли" деб белгилайди.

3.2. Криптоанализнинг автоматлашган дастурий воситасини тестлаш ва амалиётга жорий қилиш натижалари

Яратилган дастурий таъминотнинг кўриниши қуйидаги расмда тасвирланган.

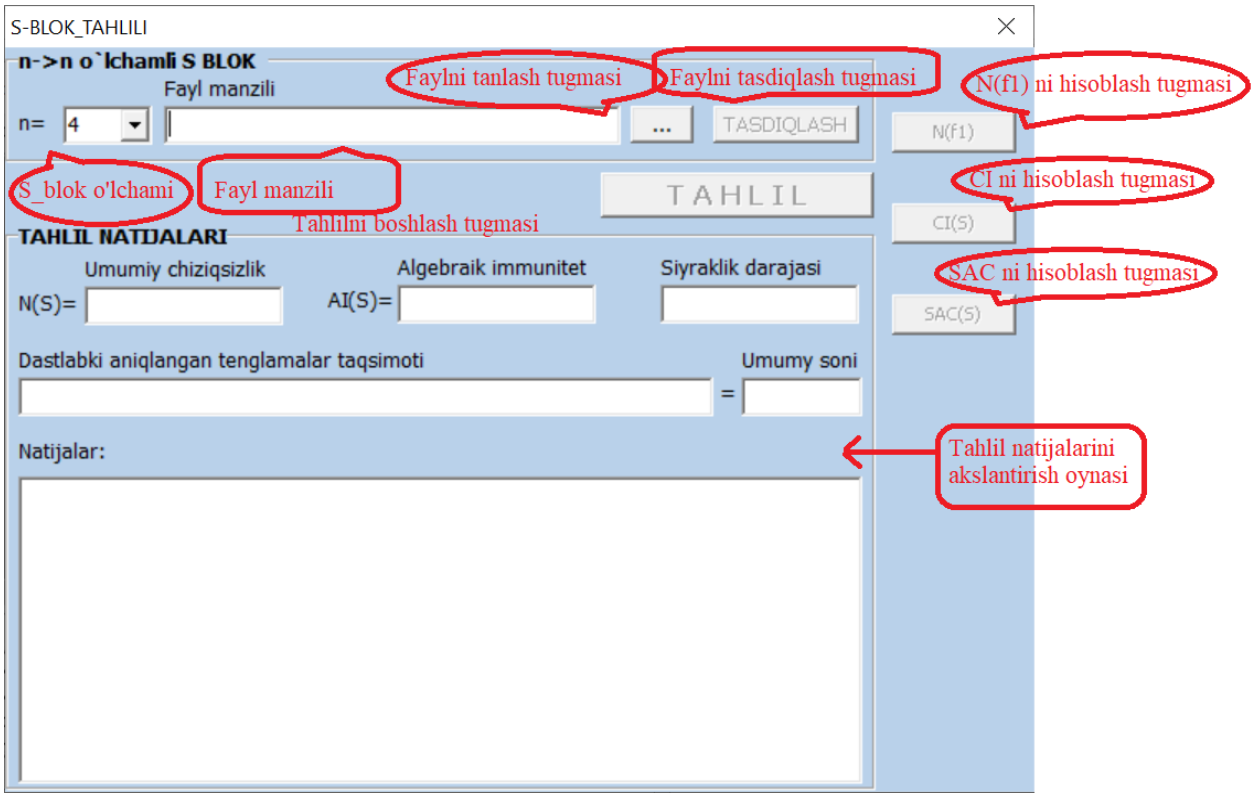


3.1-расм. S-блок таҳлили дастурий таъминоти ойнасининг кўриниши

Дастурий таъминот ёрдамида таҳлилни амалга ошириш кетма-кетлиги қуйидагича:

1. S-блок ўлчами киритилади;
2. Алмаштириш жадвали қийматлари жойлашган файлга йўл кўрсатилади;
3. “Тасдиқлаш” тугмачаси босилади;
4. “Тахлил” тугмачаси босилади;
5. “N(f1)” тугмачаси босилади;
6. “CI(S)” тугмачаси босилади;
7. “SAC(S)” тугмачаси босилади;

Қуйидаги расмда дастурий таъминот ойнасидаги бўлимлар ва тугмачаларнинг функционал вазифалари кўрсатилган:



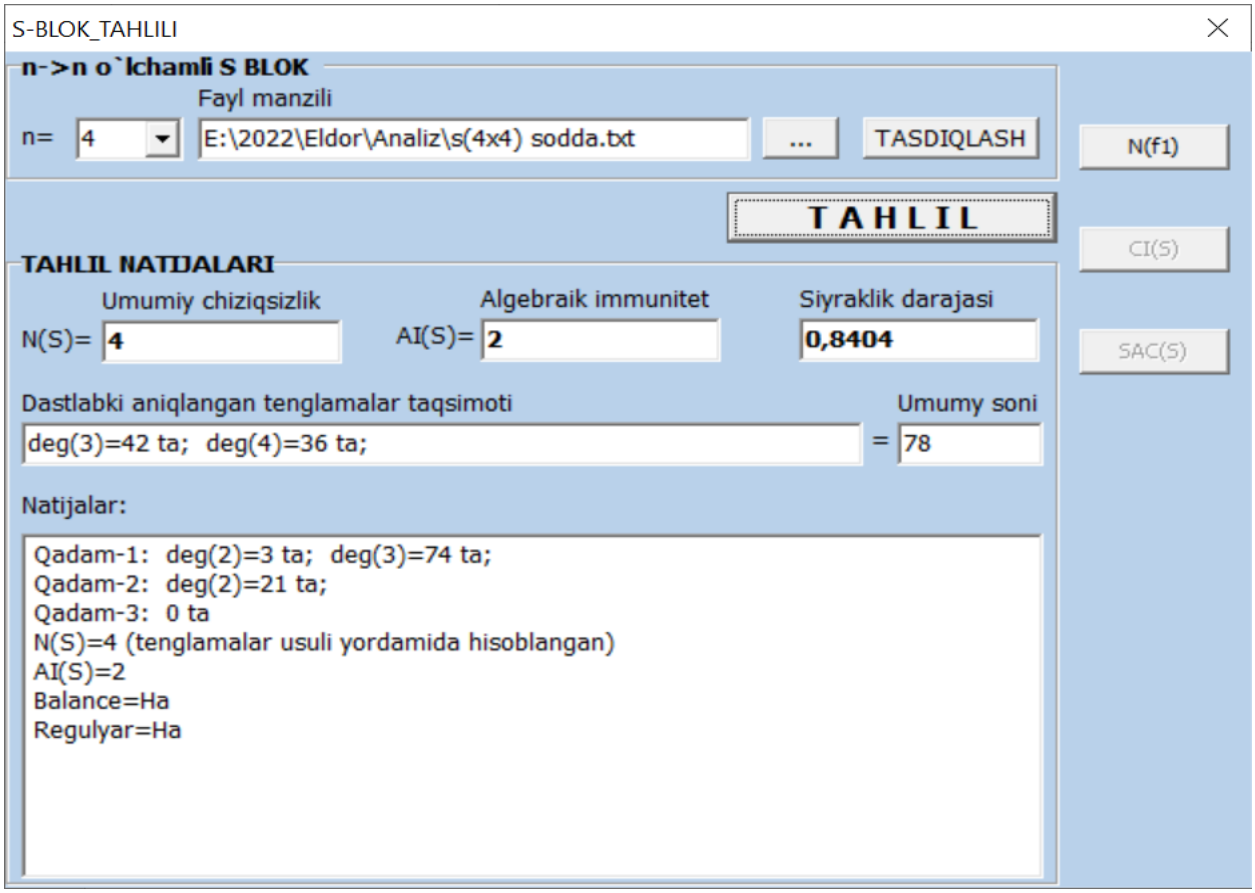
3.2-расм. Дастурий таъминот ойнаси бўлимлари

4 ўлчамли 0,4,8,13,1,5,11,6,2,14,10,3,7,9,12,15, алмаштириш жадвалининг таҳлилини амалга ошириш жараёнини кўриб чиқамиз. Файл манзили қуйидагича: E:\2022\Eldor\Analiz\s(4x4) sodda.txt.

Файл манзилини кўрсатиб “TASDIQLASH” тугмачасини босамиз.

Шундан сўнг таҳлил жараёнини бошлаш учун “TAHLIL” тугмачаси босилади.

Дастур акслантиришни ифодаловчи функцияни ифодаловчи буль тенгламалар системасини шакллантиради. Умумий чизиқсизлик, алгебраик иммунитет, Сийраклик даражалари каби параметрлар ҳисобланиб таҳлил натижаларини акслантириш ойнасида акс эттирилади.

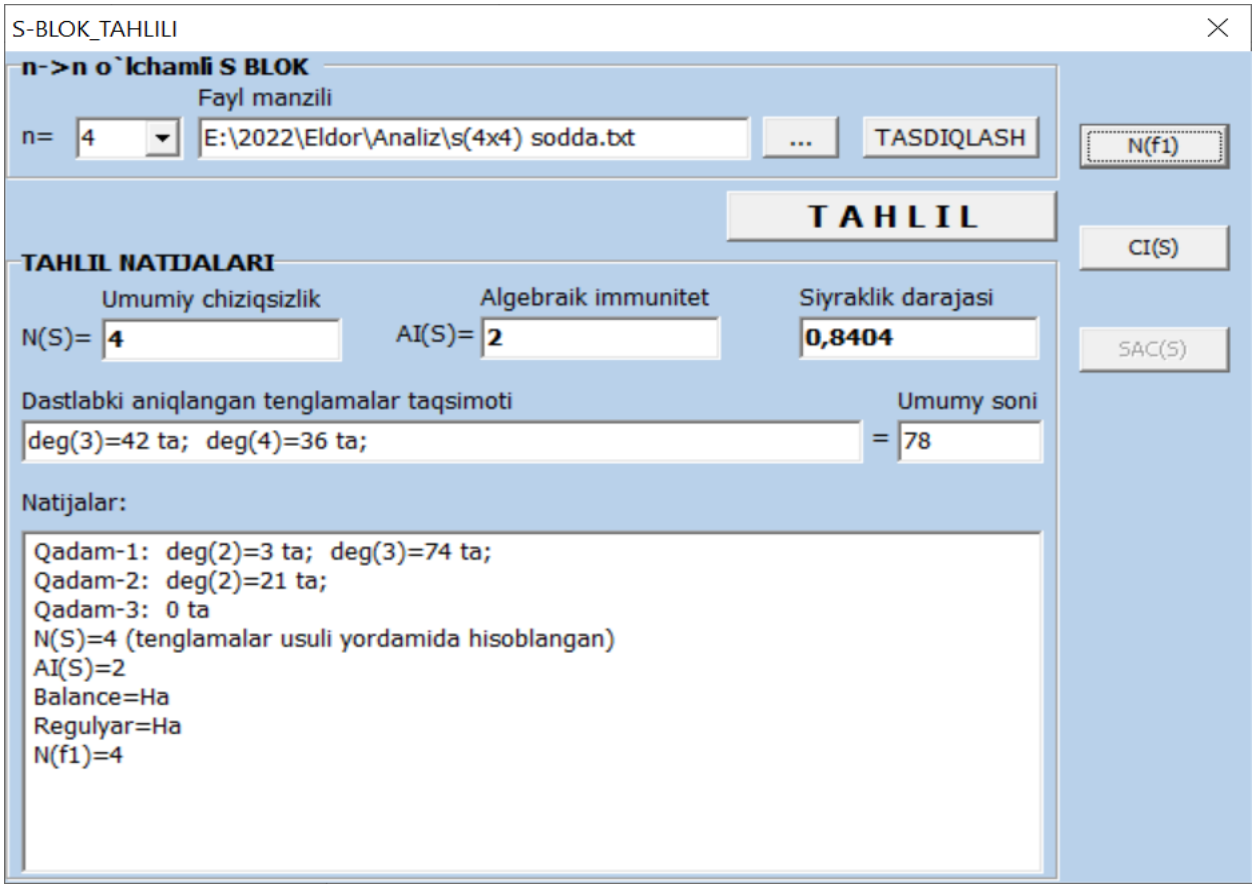


3.3-расм. Кўрсатилган s-блок акслантиришига нисбатан таҳлил жараёни натижалари

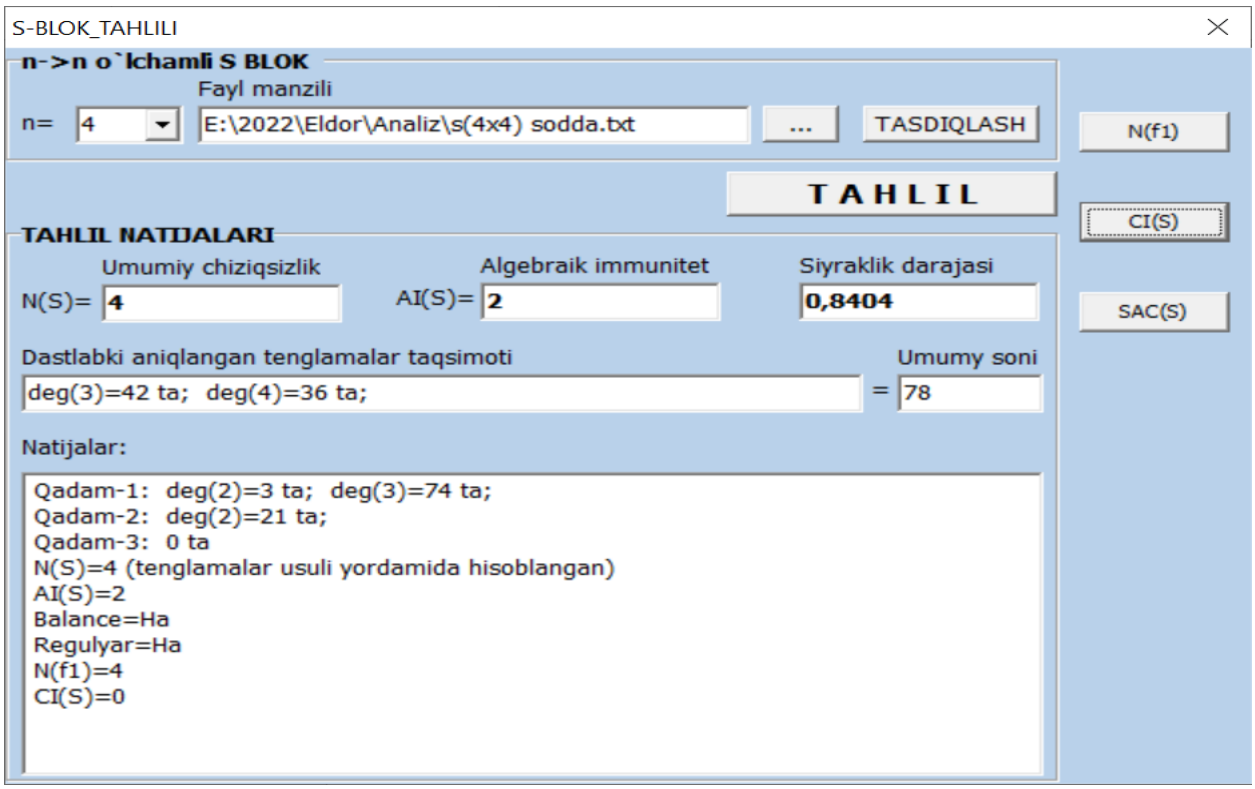
Шундан сўнг, N(f1) тугмаси босилади ва Уалш-Адамар акслантириши ёрдамида аниқланган чизиқчизлик қиймати ҳисобланади (3.4-расм).

Сўнгра CI(S) тугмасини босиш билан корреляцион иммунитет қиймати ҳисобланади (3.5-расм).

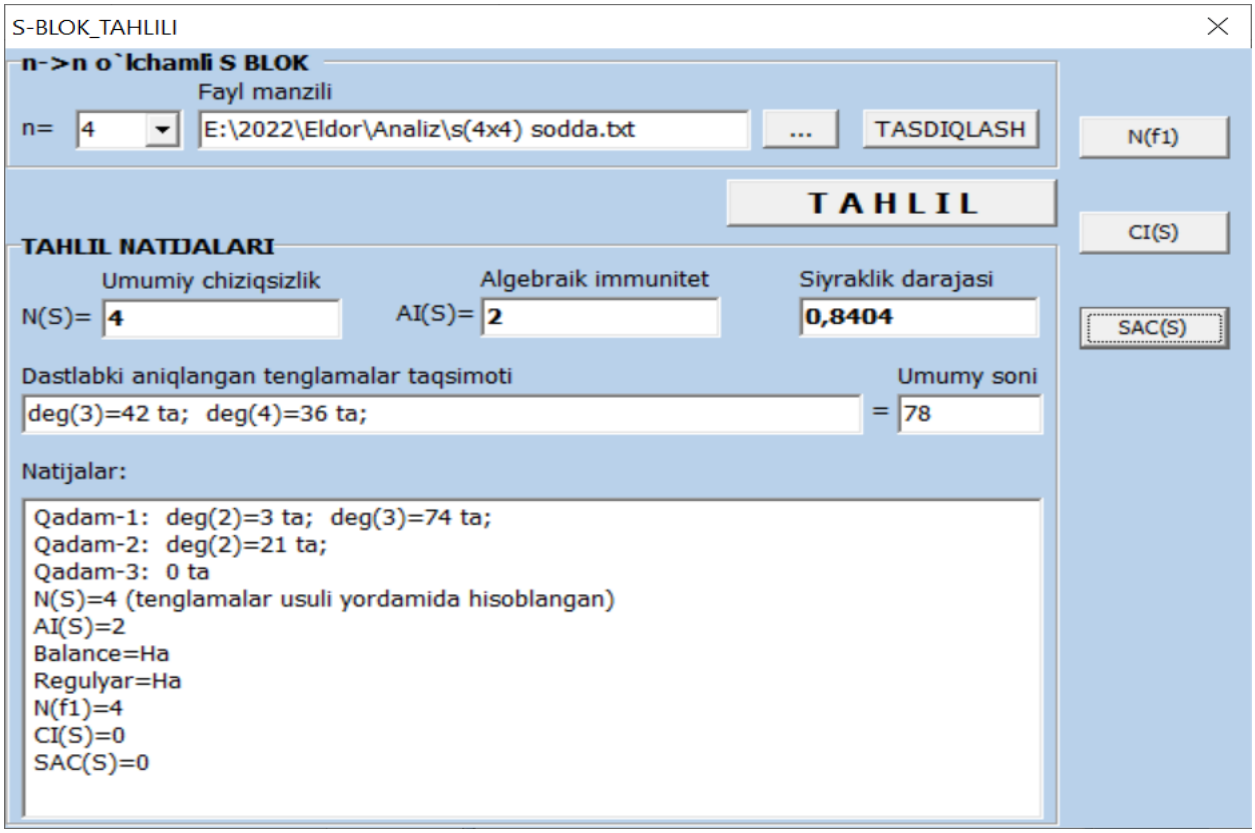
SAC(S) тугмасини босиш билан эса қатъий лавин самарадорлик аниқланади (3.6-расм).



3.4-расм. Чизиқсизлик қийматининг ҳисобланиши натижаси



3.5-расм. Корреляцион иммунитет қийматининг ҳисобланиши натижаси



3.6-расм. Қатъий лавин самарадорлик қийматининг ҳисобланиши натижаси

Дастурий таъминот ёрдамида олинган натижалар

Яратилган дастурий таъминот ёрдамида олинган айрим стандарт алгоритмларда фойдаланиладиган S-блокларнинг умумий криптографик талабларга баҳолаш натижалари қуйида келтирилган.

3.1-жадвал

Магма S_{1-4} – блокларининг криптографик талаблар бўйича баҳоси

Магма	S_1 - блок				S_2 - блок				S_3 - блок				S_4 - блок			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Баланслашганлик	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Регулярлик	+				+				+				+			
deg (f)	2	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3
N (φ)	4				4				4				4			
$CI(f)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$SAC(f)$*	+	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-
$AI(S)$	2				2				2				2			

3.2-жадвал

Магма S_{5-8} – блокларининг криптографик талаблар бўйича баҳоси

Магма	S_5 - блок				S_6 - блок				S_7 - блок				S_8 - блок			
	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Баланслашганлик	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Регулярлик	+				+				+				+			
deg (f)	2	3	3	3	2	3	3	2	2	3	3	3	3	3	3	3
N (φ)	4				4				4				4			
$CI(f)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$SAC(f)$*	-	-	-	-	-	-	-	+	+	-	-	-	-	-	+	-
$AI(S)$	2				2				2				2			

3.3-жадвал

Кузнечик алгоритми S – блокининг криптографик талаблар бўйича баҳоси

Кузнечик	S - блок							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Баланслашганлик	+	+	+	+	+	+	+	+
Регулярлик	+							
deg (f)	7	7	7	7	7	7	7	7
N (φ)	100							
$CI(f)$	0	0	0	0	0	0	0	0
$SAC(f)$*	-	-	-	-	-	-	-	+
$AI(S)$	3							

3.4-жадвал

AES шифрлаш алгоритми Sub Bytes акслантиришининг криптографик кўрсаткичлари

AES	Sub Bytes							
	f1	*f2*	*f3*	*f4*	*f5*	*f6*	*f7*	*f8*
Баланслашганлик	+	+	+	+	+	+	+	+
Регулярлик	+							
deg (f)	7	7	7	7	7	7	7	7
N (φ)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	6	8	8	8	8	6	6	6
$AI(S)$	2							

3.5-жадвал

DES алгоритми S блоклари акслантиришининг криптографик кўрсаткичлари

DES	S1	S2	S3	S4	S5	S6	S7	S8
Баланслангашл	+	+	+	+	+	+	+	+
Регулярлик	+	+	+	+	+	+	+	+
deg (f)	5	5	5	4	5	4	5	5
N (φ)	14	16	16	16	12	18	14	16
SAC(f)	8	14	12	6	10	10	12	10
$AI(S)$	2	2	2	2	2	2	2	2
$CI(f)$	0	0	0	0	0	0	0	0

3.6-жадвал

ГОСТ 28147–89 алгоритми S блоклари акслантиришининг криптографик кўрсаткичлари

ГОСТ 28147–89	S1	S2	S3	S4	S5	S6	S7	S8
Баланслашганли	+	+	+	+	+	+	+	+
Регулярлик	+	+	+	+	+	+	+	+
deg (f)	2	3	3	2	3	3	2	2
N (φ)	4	2	2	2	2	2	2	2
SAC(f)	2	2	2	4	2	4	2	2
$AI(S)$	2	2	2	2	2	2	2	2
$CI(f)$	0	0	0	0	0	0	0	0

3.7-жадвал

O’zDst 1105:2009 алгоритми BaytAlmash акслантириши учун стандартда келтирилган калит ёрдамида генерация қилинган S_1 – блокнинг криптографик кўрсаткичлари

O’zDst 1105:2009	S1 блок							
	f1	f2	f3	f4	f5	f6	f7	f8
баланслашганлик	+	+	+	+	+	+	+	+

регулярлик	+	+	+	+	+	+	+	+
deg (f)	7	7	7	7	7	7	7	7
N (f)	112	112	112	112	112	112	112	112
N (φ)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	6	6	6	8	2	4	8	8

3.8-жадвал

O’zDst 1105:2009 алгоритми BaytAlmash акслантириши учун стандартда келтирилган калит ёрдамида генерация қилинган S_2 – блокнинг криптографик кўрсаткичлари

O’zDst 1105:2009	Генерация қилинган S2 блок							
	f1	f2	f3	f4	f5	f6	f7	f8
баланслашганлик	+	+	+	+	+	+	+	+
регулярлик	+	+	+	+	+	+	+	+
deg (f)	7	7	7	7	7	7	7	7
N (f)	112	112	112	112	112	112	112	112
N (φ)	112							
CI(f)	0	0	0	0	0	0	0	0
SAC(f)	6	6	6	6	6	6	4	4

Боб бўйича хулосалар

Ушбу бобда симметрик блокли шифрлаш алгоритмларининг S-жадвал(лар)и (субституция блоклари) ни криптографик талабларга мувофиқлигини баҳолаш учун автоматлаштирилган дастурий восита ишлаб чиқиш масалалари ёритилди.[43]

Ишлаб чиқилган дастурий комплекс қуйидаги асосий криптографик хусусиятларни ҳисоблаш ва таҳлил қилиш имконини берди:

- *Чизиқсизлик даражаси* (Nonlinearity – N(S)) – тенгламалар усули (алгебраик нормал шакл – АНФ) ёрдамида ҳисобланган;
- *Алгебраик иммунитет* (Algebraic Immunity – AI(S)) – даражани босқичма-босқич пасайтириш орқали аниқланган;
- *Сийраклик* (Sparsity) – АНФ даги бирҳадлар сони асосида баҳоланган;
- *Баланслашганлик* (Balance) – чиқиш векторининг 0 ва 1 лар сони тенглиги текширилган;

- Completeness (Тўлиқлик – CI) – ҳар бир кириш битининг чиқишга таъсири;
- Strict Avalanche Criterion (SAC) – бит ўзгаришининг қаттиқ лавинавий тарқалиши шартлари.

Дастур қуйидаги функционал имкониятларга эга бўлди:

- 4×4 дан 8×8 гача ўлчамдаги S-блокларни қўллаб-қувватлаш;
- Матн файлидан S-жадвални ўқиш ва автоматик таҳлил қилиш;
- Ҳар бир босқичда оралиқ натижаларни (АНФ, даражалар, бирҳадлар сони) кўрсатиш ва файлга сақлаш.[47]

- Натижаларни визуал ва матн шаклида (Memo, LabeledEdit майдонлари ва алоҳида .txt файл) тақдим этиш.
- Тестлаш жараёнида турли ўлчамдаги (асосан 4×4, 6×6, 8×8) маълум S-блоклар (шу жумладан AES, PRESENT, магистрал алгоритмларнинг S-қутилари ва тасодифий генерация қилинган жадваллар) устида синовдан ўтказилди. Олинган натижалар қуйидагиларни тасдиқлади:

Ишлаб чиқилган восита S-блокларнинг криптографик мустаҳкамлигини баҳолашда етарли аниқлик ва самарадорликка эга;

Ҳисоблаш мураккаблиги ўлчам ошгани сари кескин ортиши (айниқса 7×7 ва 8×8 учун) кузатилди, лекин 6×6 гача бўлган жадваллар учун амалий вақт ичида (бир неча сония – бир неча дақиқа) натижа беради;

- Энг юқори чизиқсизлик, алгебраик иммунитет ва SAC кўрсаткичларига эга S-блоклар замонавий блок шифрлари талабларига мос келиши аниқланди;
- Восита янги S-жадвалларни яратиш ва танлаш жараёнида крипто-муҳандис сифатида фойдали ёрдамчи восита бўла олишини исботлади.

Шундай қилиб, III бобда ишлаб чиқилган автоматлаштирилган дастурий восита симметрик блокли шифрлаш алгоритмлари лойиҳалаш ва уларнинг криптобардошлилигини дастлабки баҳолаш босқичида муҳим амалий аҳамиятга эга эканлиги кўрсатилди. Ушбу восита Ўзбекистон шароитида миллий криптографик алгоритмларни ишлаб чиқиш ва халқаро стандартларга мувофиқлигини текширишда қўлланилиши мумкин.

Кейинги тадқиқотларда дастурни янада оптималлаштириш, параллел ҳисоблашни жорий этиш, каттароқ ўлчамдаги (≥8 бит) жадвалларни таҳлил қилиш имкониятини кенгайтириш ва дифференциал/чизиқли хусусиятларни қўшимча баҳолаш модулларини қўшиш бўйича ишлар давом эттирилиши мумкин.

3.3.Миллий ва халқаро шифрлаш стандартлари S-блокларининг қиёсий таҳлили.

Замонавий блокли шифрлаш стандартларининг хавфсизлик даражаси уларда қўлланиладиган S-блокларнинг криптографик хусусиятлари билан белгиланади. Ушбу бўлимда Ўзбекистон Республикаси давлат стандарти **O‘zDSt 1105:2009**, АҚШ стандарти **AES (FIPS 197)** ва Россия Федерацияси стандарти **GOST 34.12-2015 (Kuznyechik)** алгоритмларидаги S-блокларнинг қиёсий таҳлили келтирилган.

3.3.1. Стандартларда қўлланиладиган S-блокларнинг конструктив хусусиятлари.

Криптографик алгоритмларнинг хавфсизлигини таъминлашда S-блоклар (алмаштириш жадваллари) ягона чизиқли бўлмаган компонент ҳисобланади. Уларнинг асосий вазифаси — шифрланаётган маълумот ва калит ўртасидаги боғлиқликни мураккаб («confusion» – адаштириш) қилишдир.

1. S-блокларнинг асосий конструктив турлари

Замонавий стандартларда S-блокларни яратишда икки хил асосий ёндашувдан фойдаланилади:

Алгебраик (Математик) ёндашув: S-блоклар чекли майдонлардаги ($\boldsymbol{GF(2^n)}$) математик амаллар, масалан, тескари элементни топиш x^{-1} асосида қурилади.

Мисол: AES (Rijndael) стандарти.

Эвристик ёки Тасодифий ёндашув: S-блоклар махсус қидирув алгоритмлари ёки тасодифий генерация ёрдамида яратилиб, кейин криптографик мезонларга мувофиқлиги текширилади.[13]

Мисол: DES, PRESENT (енгил вазнли шифрлар).

2. Муҳим конструктив кўрсаткичлар.

Стандартларда қўлланиладиган S-блоклар қуйидаги конструктив хусусиятларга эга бўлиши шарт:

Дифференциал бир хиллик $\boldsymbol{\delta}$: Кириш ва чиқиш дифференциаллари ўртасидаги боғлиқлик минимал бўлиши керак. Масалан, AES учун $\delta = 4$, кўплаб енгил вазнли шифрларда эса бу қиймат 4 ёки 2 (APN) га тенг.

Чизиқли бўлмаганлик (Nonlinearity): S-блокнинг чизиқли функциялардан максимал даражада узоқлиги. Бу кўрсаткич қанча юқори бўлса, чизиқли криптотаҳлилга қаршилик шунча кучли бўлади.

Кўчки эффекти (Avalanche effect): Киришдаги битта битнинг ўзгариши чиқишдаги камида ярим битларнинг ўзгаришига олиб келиши керак.[65]

Алгебраик даража: S-блокни ифодаловчи Буль функциясининг даражаси юқори бўлиши керак (масалан, n-1).

3. Турли стандартлардаги S-блокларнинг таҳлили

Стандарт / Алгоритм	Конструкция тури	Ўлчами (бит)	Хусусияти
AES (FIPS 197)	Алгебраик ($\boldsymbol{x^{-1}}$ + аффин алмаштириш)	8x8	Юқори чизиқли бўлмаганлик, аппаратда амалга ошириш бироз мураккаб.
PRESENT	Эвристик (Оптималлаштирилган)	4x4	Аппарат воситаларида (FPGA/ASIC) минимал ресурс сарфлайди.
O‘zDSt 1105	Аралаш / Динамик ёки Статик	8x8	Миллий стандартда турли хил алмаштириш жадвалларидан фойдаланиш имкони мавжуд.
Ascon	Алгебраик (SPN-тармоғи учун)	5x5	Енгил вазнли ва бит-селайсинг (bit-slicing) учун қулай.

4. Конструкциянинг амалий аҳамияти

S-блокларнинг конструктив тузилиши алгоритмнинг ишлаш тезлигига ҳам таъсир қилади:

- **Математик қурилган блоклар** алгоритмни тасвирлашда ихчам бўлсада, аппаратда қўшимча ҳисоблашларни талаб қилиши мумкин.
- **Қидирув асосида қурилган** (4-битли) блоклар IoT қурилмалари ва ресурс чекланган муҳитлар (масалан, ESP32 ёки Arduino) учун энг мақбул ечим ҳисобланади.[65]

3.3.2. Қиёсий таҳлил натижалари

Замонавий блокли шифрлаш алгоритмларида қўлланиладиган S-блокларнинг самарадорлиги уларнинг криптографик мустаҳкамлиги ва аппарат воситаларида амалга оширилиш ресурслари билан белгиланади. Қуйида асосий алгоритмларнинг S-блоклари бўйича қиёсий таҳлил натижалари келтирилган.

1. Криптографик кўрсаткичлар қиёси:S-блокларнинг чизиқли бўлмаганлик (NL) ва дифференциал бир хиллик $\boldsymbol{\delta}$ кўрсаткичлари уларнинг математик ҳужумларга бардошлилигини ифодалайди.

3.3.2-жадвал

Алгоритм (S-блок)	Ўлчами (бит)	Дифференциал бир хиллик δ)	Чизиқли бўлмаганлик (NL)
AES (Rijndael)	8x8	4	112
PRESENT	4x4	4	4
Ascon	5x5	8	12
O‘zDSt 1105	8x8	4-6	104-110
CLEFIA	8x8	4	112

Таҳлил: * AES энг юқори чизиқли бўлмаганлик (NL=112) кўрсаткичига эга бўлиб, чизиқли криптотаҳлилга максимал чидамлиликни таъминлайди.

PRESENT енгил вазнли алгоритм бўлишига қарамай, ўз ўлчами (4-бит) учун оптимал $\delta = 4$ кўрсаткичини сақлаб қолган.

2. Аппарат воситаларида амалга ошириш самарадорлиги: Ресурс чекланган қурилмаларда (IoT, сенсор тармоқлари) S-блокнинг эгаллаган майдони (GE - Gate Equivalents) муҳим аҳамиятга эга.

Алгоритм	Амалга ошириш усули	Майдон (GE)	Энергия сарфи
AES	Lookup Table (LUT)	~800+	Юқори
PRESENT	Combinational Logic	~28	Жуда паст
Ascon	Bit-slicing	~60-80	Паст
GIFT	Logic Gates	~25	Минимал

Хулоса: Енгил вазнли шифрлар (PRESENT, GIFT) S-блоклари AES-га қараганда аппаратда **20-30 баравар** кам жой эгаллайди. Бу уларни кичик микроконтроллерлар ва RFID-тегларда қўллаш имконини беради.

Дифференциал ва чизиқли таҳлилга чидамлилик нисбати

Қиёсий таҳлил натижалари шуни кўрсатадики:

AES S-блоклари алгебраик жиҳатдан мураккаб бўлиб, катта ҳажмдаги маълумотларни ҳимоя қилиш учун мос келади.[13]

PRESENT ва шу каби 4-битли блоклар дифференциал бир хиллик бўйича яхши натижа берса-да, уларнинг чизиқли бўлмаганлиги паст. Шу сабабли, хавфсизликни таъминлаш учун уларда раундлар (итерациялар) сони кўпроқ қилиб белгиланади (масалан, 31 раунд).

Ascon алгоритмида қўлланиладиган 5-битли S-блок махсус "Bit-slicing" технологияси учун оптималлаштирилган бўлиб, у дастурий ва аппарат воситалари ўртасида мувозанатни таъминлайди.

Боб юзасидан хулоса

Ушбу бобда амалга оширилган тадқиқотлар ва дастурий ишланмалар натижасида қуйидаги муҳим илмий ва амалий хулосаларга келинди:

Автоматлаштирилган таҳлил тизими: Симметрик блокли шифрлаш алгоритмларининг асосий ночизиқли компоненти бўлган S-блокларни комплекс баҳолаш имконини берувчи дастурий мажмуа ишлаб чиқилди. Ушбу восита Borland Delphi муҳитида реализация қилинган бўлиб, у криптотаҳлил жараёнларини соддалаштириш ва инсон омили хатоларини минималлаштиришга хизмат қилади.

Криптографик кўрсаткичлар таҳлили: Ишлаб чиқилган дастурий восита ёрдамида S-блокларнинг баланслашганлик, чизиқсизлик даражаси (Nonlinearity), алгебраик иммунитет ва қатъий лавин самарадорлиги (SAC) каби фундаментал кўрсаткичларини ҳисоблаш алгоритмлари оптималлаштирилди. Хусусан, Уолш-Адамар алмаштириши ва Хеминг масофасини ҳисоблаш модулларининг дастурий реализацияси ҳисоблаш тезлигини ошириш имконини берди.

Қиёсий таҳлил натижалари: Мавжуд халқаро стандартлар (AES, PRESENT, ASCON) ва миллий шифрлаш алгоритмларининг S-блоклари қиёсий таҳлил қилинди. Натижалар шуни кўрсатдики, AES алгоритми энг юқори чизиқсизлик кўрсаткичига (NL=112) эга бўлса, PRESENT ва ASCON каби енгил вазнли алгоритмлар ресурс чекланган муҳитлар учун оптимал хавфсизлик ва самарадорлик мувозанатини таъминлайди.

Амалий аҳамият: Тадқиқот давомида аниқландики, енгил вазнли шифрларнинг (PRESENT, GIFT) S-блоклари аппарат воситаларида (IoT ва сенсор тармоқлари) амалга оширишда анъанавий AES алгоритмига

нисбатан 20-30 баравар кам майдон (GE) эгаллайди. Бу эса ишлаб чиқилган дастурий воситадан янги авлод шифрларини лойиҳалашда энг мақбул S-блок конфигурацияларини танлашда самарали фойдаланиш мумкинлигини исботлайди.[75,77]

Истиқболли йўналишлар: Ишлаб чиқилган автоматлаштирилган дастурий восита нафақат мавжуд алгоритмлар аудити учун, балки янги миллий криптографик стандартларни яратиш ва уларнинг бардошлилигини математик исботлаш жараёнида мустаҳкам пойдевор бўлиб хизмат қилади.

УМУМИЙ ХУЛОСАЛАР

Монография ишида “Криптотаҳлилнинг автоматлаштирилган дастурий воситаларини ишлаб чиқиш” мавзусида олиб борилди ва симметрик блокли шифрлаш алгоритмларининг криптобардошлилигини баҳолашнинг муҳим жиҳатларига бағишланди.

Ишнинг асосий мақсади — симметрик блокли шифрлаш алгоритмларининг асосий компонентларидан бири бўлган S-жадваллар (субституция блоклари) ни криптографик талабларга мувофиқлигини автоматик равишда текшириш ва баҳолаш имконини берувчи дастурий воситани ишлаб чиқишдан иборат эди.

Тадқиқот давомида қуйидаги асосий натижаларга эришилди: Симметрик ва асимметрик шифрлаш алгоритмларини криптотаҳлил қилишнинг классик ва замонавий усуллари (тўлиқ танлаш, дифференциал ва чизиқли таҳлил, частотавий таҳлил, алгебраик ҳужумлар ва бошқалар) тизимли равишда ўрганилди ва таҳлили берилди.Симметрик блокли шифрлаш алгоритмларининг криптомустаҳкамлигини таъминловчи асосий омиллардан бири — S-жадвалларнинг хусусиятлари (чизиқсизлик, алгебраик иммунитет, баланслашганлик, тўлиқлик, strict avalanche criterion, сийраклик ва бошқалар) батафсил кўриб чиқилди.

Ушбу хусусиятларни ҳисоблаш ва баҳолаш учун Delphi муҳитида автоматлаштирилган дастурий восита ишлаб чиқилди. Дастур қуйидаги имкониятларга эга:

- 4×4 дан 8×8 гача ўлчамдаги S-жадвалларни қўллаб-қувватлаш;
- Алгебраик нормал шакл (ANF) орқали чизиқсизлик ва алгебраик иммунитетни ҳисоблаш;
- Босқичма-босқич даражани пасайтириш усули билан аниқ натижаларга эришиш;

- Баланслашганлик, тўлиқлик (CI), SAC ва сийраклик кўрсаткичларини автоматик аниқлаш;
- Натижаларни матнли файлга сақлаш ва фойдаланувчи интерфейси орқали визуал кўрсатиш.

Ишлаб чиқилган восита турли S-жадваллар (шу жумладан AES, PRESENT ва бошқа маълум алгоритмларнинг S-блоклари, шунингдек тасодифий генерация қилинган жадваллар) устида синовдан ўтказилди. Натижалар дастурнинг етарли аниқлик ва амалий самарадорликка эга эканлигини тасдиқлади. Айниқса, 6×6 гача бўлган ўлчамлар учун ҳисоблаш вақти қабул қилинадиган даражада бўлиб, крипто-муҳандислик амалиётида қўллаш мумкинлиги исботланди. Ишнинг илмий янгилиги шундаки, Ўзбекистон шароитида симметрик блокли шифрлаш алгоритмлари учун S-жадвалларни бир нечта криптографик мезонлар бўйича бир вақтда баҳолайдиган автоматлаштирилган дастурий восита биринчи марта ишлаб чиқилди ва амалий синовдан ўтказилди.[46]

Амалий аҳамияти: яратилган дастурий восита

- миллий криптографик алгоритмларни лойиҳалаш ва баҳолашда,
- мавжуд алгоритмларнинг S-блокларини халқаро стандартларга мувофиқлигини текширишда,
- ўқув ва илмий-тадқиқот жараёнларида фойдали ёрдамчи восита сифатида қўлланилиши мумкин.

Хулоса қилиб айтганда, диссертация иши криптотаҳлил соҳасидаги автоматлаштириш даражасини оширишга қаратилган бўлиб, симметрик блокли шифрлаш алгоритмларининг ишончлилигини баҳолашда муҳим натижаларга эришди. Олинган натижалар ва ишлаб чиқилган дастурий восита келгусида миллий криптотизимларни яратиш, такомиллаштириш ва хавфсизлик стандартларига мувофиқлигини таъминлаш йўналишида қўлланилиши мумкин бўлган мустаҳкам асос бўлиб хизмат қилади.

Кейинги тадқиқотларда дастурни оптималлаштириш, параллел ҳисоблаш технологияларини жорий этиш, каттароқ ўлчамдаги S-жадвалларни таҳлил қилиш имкониятини кенгайтириш, шунингдек дифференциал ва чизиқли хусусиятларни қўшимча баҳолаш модулларини интеграция қилиш бўйича ишлар давом эттирилиши тавсия этилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Арипов М.М., Пудовченко Ю.Е. Основы криптологии. - Ташкент: 2004. – 136 с.
2. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.
3. Алексеев А. Криптография и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html.
4. Бияшев Р.Г., Горковенко Е.В., Нысаанбаева С.Е. Алгоритмы шифрования сообщений и формирования электронной цифровой подписи с заданной криптостойкостью информации // Институт проблем информатики и управления МОН РК, г. Алма-Ата.
5. Защита информации. Малый тематический выпуск ТИИЭР. – Москва, 1988. – т.76, №5.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
7. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.
8. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004.
9. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд.: Лори Вильямс, 2001.
10. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005.
11. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.
12. Авдошин С.М., Савельева А.А. «Криптоанализ: вчера, сегодня, завтра», Государственный университет – Высшая Школа Экономики. Москва – 2007.

13. Авдошин С.М., Савельева А.А. «Криптоанализ: савременное состояние и перспективы развития», Государственный университет – Высшая Школа Экономики.

14. Жуков А.Е. «Криптоанализ по побочным каналам (Side Channel Attacks)», Пособие по курсу «Криптографические методы защиты информации» Москва – 2004.

15. Joux, Antoine. Algorithmic cryptanalysis / Antoine Joux. p. cm. -- (Chapman & Hall/CRC cryptography and network security) Includes bibliographical references and index, 2009.

16. Кузнецов М.И., Бурланков Д.Е., Чирков А.Ю., Яковлев В.А. Компьютерная алгебра: Учебник. // Нижегородский Государственный Университет им. Н.И. Лобачевского, 2002. опубликовано: http://www.itlab.unn.ru/archive/docs/coaBook.pdf.

17. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

18. О.М. Алланов, Э.И. Саидахмедов. Симметрик блокли шифрлаш алгоритмларига қўлланилувчи криптотаҳлил усули. Электр энергетикаси таъминоти тизими узлуксизлигини таъминлаш долзарб муаммоларининг самарадор ечимлари. Республика илмий техник – анжумуни. Фарғона 2021 йил. 166-169 б.

19. О.М. Алланов, Э.И. Саидахмедов. Симметрик блокли шифрлаш алгоритмларига қўлланилувчи криптотаҳлил усуллари. Иқтисодиёт тармоқларининг инновацион ривожланишида ахборот-коммуникация технологияларининг аҳамияти. Республика илмий-техник анжумани. Тошкент 2021 йил. 347-349 б.

20. https://www.keylength.com/en/compare/#Biblio7

21. Arjen K. Lenstra and Eric R. Verheul. Selecting Cryptographic Key Sizes, Journal Of Cryptology, vol. 14, p. 255-293, 2001.

22. Arjen K. Lenstra, Key Lengths. The Handbook of Information Security, 06/2004.

23. Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014.

24. Commercial National Security Algorithm, National Security Agency (NSA), 01/2016.

25. Determining Strengths for Public Keys Used for Exchanging Symmetric Keys, RFC 3766, H. Orman and P. Hoffman, 04/2004

26. Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020

27. Ғаниев С.К., Каримов М.М., Ташев К.А. Криптографик усуллар. – Тошкент: Алоқачи, 2011. – 540 б.

28. Алматов Ж. Ахборот хавфсизлиги. – Тошкент: Фан ва технология, 2012.

29. Каримов М.М. Ахборот хавфсизлиги ва криптография. – Тошкент, 2018

30. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Ed. – Pearson, 2020

31. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1996.

32. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. – Springer, 1993.

33. Matsui M. Linear Cryptanalysis Method for DES Cipher. – EUROCRYPT '93, 1993.

34. Nyberg K. Differentially uniform mappings for cryptography. – EUROCRYPT ’93, pp. 55–64, 1994.

35. Bogdanov A., et al. PRESENT: An Ultra-Lightweight Block Cipher. – CHES 2007, pp. 450–466

36. Dobraunig C., et al. Ascon v1.2: Lightweight Cryptography for the 21st Century. – 2021.

37. Guo J., et al. The LED Block Cipher. – CHES 2011, LNCS 6917, pp. 326–341.

38. Borghoff J., et al. PRINCE – A Low-latency Block Cipher. – ASIACRYPT 2012

39. Ғаниев С.К., Ғаниева З.А. Ахборот хавфсизлиги. Криптография асослари. – Тошкент: “Fan va texnologiya”, 2019.

40. Худойқулов З.Т. Маълумотларни шифрлашнинг замонавий алгоритмлари ва уларнинг криптобарқарорлиги. – Тошкент, 2020.
41. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes. – Cambridge University Press, 2021. – 720 p.
42. NIST Special Publication 800-225. Submission Requirements and Evaluation Process for the Lightweight Cryptography Standardization Process. – NIST, 2019.
43. Beaulieu R., et al. The SIMON and SPECK Families of Lightweight Block Ciphers. – IACR Cryptology ePrint Archive, 2013.
44. Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. – Springer, 2002.
45. Boura C., Canteaut A. On the Influence of the Initial Permutation on the Confusion and Diffusion Properties of Block Ciphers. – Journal of Cryptology, 2016.
46. Moura L., Bjørner N. Z3: An Efficient SMT Solver. – Tools and Algorithms for the Construction and Analysis of Systems, 2008.
47. Sun S., et al. Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SNOW, SIMON, and SPECK. – CRYPTO, 2014.
48. National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication (FIPS) 197: Advanced Encryption Standard (AES). – 2001.
49. Knudsen L.R., Robshaw M. The Block Cipher Companion. – Springer-Verlag Berlin Heidelberg, 2011.
50. Banik S., et al. GIFT: A Small Present. – CHES 2017, LNCS 10529, pp. 321–345, 2017.
51. ISO/IEC 29192-2:2019. Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers.
52. Jean J. TikZ for Cryptographers. – [Elektron resurs]. URL: https://www.iacr.org/authors/tikz/
53. Huwyler C. Analysis of Lightweight Cryptographic Algorithms for IoT Devices. – University of Zurich, 2020.

54. Shibutani K., et al. Piccolo: An Ultra-Lightweight Block Cipher. – CHES 2011, LNCS 6917, pp. 342–357, 2011.
55. Guo J., et al. The PHOTON Family of Lightweight Hash Functions. – CRYPTO 2011, LNCS 6841, pp. 222–239, 2011.
56. Hell M., Johansson T., Meier W. Grain: A Stream Cipher for Constrained Environments. – International Journal of Wireless and Mobile Computing, 2007.
57. Gong G., et al. Warbler: A Lightweight Block Cipher for RFID Tags. – 2014.
58. Cannière C., Dunkelman O., Knežević M. KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. – CHES 2009, LNCS 5747, pp. 272–288, 2009.
59. Suzaki K., et al. TWINE: A Lightweight Block Cipher for Multiple Platforms. – SAC 2012, LNCS 7707, pp. 339–354, 2013.
60. Wenling Wu, Lei Zhang. LBlock: A Lightweight Block Cipher. – ACNS 2011, LNCS 6715, pp. 327–344, 2011.
61. Hämäläinen P., et al. Design and Implementation of Low-Area and Low-Power AES. – IEEE Transactions on VLSI Systems, 2006.
62. Bogdanov A., et al. SPONGENT: A Lightweight Hash Function. – CHES 2011, LNCS 6917, pp. 312–325, 2011.
63. NIST. Announcing Request for Candidate Algorithms for the Lightweight Cryptography Standardization Process. – 2018.
64. Biryukov A., Perrin L. State of the Art in Lightweight Symmetric Cryptography. – Cryptology ePrint Archive, Report 2017/511.
65. Baksi A. A Survey on Automated Techniques for Cryptanalysis. – IEEE Access, 2021.
66. Todo Y. Integral Cryptanalysis on Full MISTY1. – CRYPTO 2015, LNCS 9215, pp. 413–432, 2015.
67. Beierle C., et al. Skinny and Mantis: A Family of Lightweight Block Ciphers and a Low-latency Lightweight Tweakable Block Cipher. – CRYPTO 2016.
68. Armknecht F., et al. Memory-Efficient Algorithms for the Middle-Prime Attack. – Journal of Cryptology, 2015.

69. Sato S., et al. Hardware Implementations of NIST Lightweight Cryptography Finalists. – 2022.
70. Ganea M.N., et al. Comparative Analysis of Lightweight Cryptography Algorithms for IoT. – IEEE Conference, 2023.
71. Wang N., et al. SAT-based Automated Differential Cryptanalysis. – 2020.
72. NIST Computer Security Resource Center. Lightweight Cryptography Project. URL: https://csrc.nist.gov/projects/lightweight-cryptography
73. IACR Cryptology ePrint Archive. URL: https://eprint.iacr.org/
74. Keylength - Cryptographic Key Length Recommendation. URL: https://www.keylength.com/
75. Ascon Official Website. URL: https://ascon.isec.tugraz.at/
76. GitHub - Ascon Lightweight Cryptography Implementation. URL: https://github.com/ascon/ascon-c
77. Lightweight Cryptography for the Internet of Things. URL: https://www.lightweightcrypto.org/
78. BSI - Cryptographic Mechanisms: Recommendations and Key Lengths. TR-02102. URL: https://www.bsi.bund.de/
79. ECRYPT-CSA. Algorithms, Key Size and Protocols Report. – 2018.
80. OpenSSL Cryptography and SSL/TLS Toolkit. URL: https://www.openssl.org/

МУНДАРИЖА

Таклиф ва тавсиялар учун

З.Т.ХУДОЙҚУЛОВ, Э.И.САИДАХМЕДОВ

КРИПТОТАҲЛИЛНИНГ АВТОМАТЛАШГАН ДАСТУРИЙ ВОСИТАЛАРИНИ ИШЛАБ ЧИҚИШ

МОНОГРАФИЙА

Техник муҳаррир: Эшқораев С. С.

Мусаҳҳиҳ: Жавгашев Й. Ж.

Тасдиқнома № 255979, 13.04.2024

Босишга 18.04.2026 да рухсат берилган. Формат 60x84/16.

Гарнитура Тимес Нew Роман. Адади 70 дона. Буюртма № 763

“Termiz publishing center” нашриётида тайёрланди ва чоп этилди.

Сурхондарё вилояти, Термиз шаҳри, Увайсий кўчаси 8А-уй, Тошкент ш.,

"ТРАСТБАНК" ХА БАНКИНИНГ БОШ ОФИСИ, МФО: 00491, ИНН:

311209934 Ҳ/Р: 20208000307031406001

Телефон: +998-88-808-21-07

ISBN 978-9910-13-276-6

9 789910 132766

6716

TERMIZ PUBLISHING CENTER

Termiz –“Termiz publishing center”-2026