ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ФАН-ТЕХНИКА ВА МАРКЕТИНГ ТАДҚИҚОТЛАРИ МАРКАЗИ

Хасанов Хислат Пўлатович

ТАКОМИЛЛАШГАН ДИАМАТРИЦАЛАР АЛГЕБРАЛАРИ ВА ПАРАМЕТРЛИ АЛГЕБРА АСОСИДА КРИПТОТИЗИМЛАР ЯРАТИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

ТОШКЕНТ
ФТМТМ
2008

УДК 681.3

Масъул муҳаррирлар:
т.ф.д., проф. С.С. Қосимов, т.ф.н. М.М. Маҳмудов

Тақризчилар:
**т.ф.д., проф. М.М. Каримов, т.ф.н., доц. Р.И. Исаев,
т.ф.н., доц. Р.В. Қобулов**

Хасанов Хислат Пўлатович
Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари — Тошкент, 2008 — 208 бет.

Ушбу китобда криптография соҳасидаги етакчи давлатлар — АҚШ, Россия ва Европа мамлакатлари давлат стандартлари ва алгоритмлари билан бир қаторда, ҳозирги кунда энг кўп қўлланиладиган, энг ишончли деб тан олинган криптографик алгоритмларни яратишга асос бўлган умумий ёндашувлар, алгебраик структуралар ва функциялар баён этилган.

Китобда такомиллашган диаматрицалар алгебраси ва параметрли алгебраларни келтириб чиқариш, улар асосида янги криптоалгоритмлар яратиш ва мавжуд криптоалгоритмларни такомиллаштиришнинг умумий усуллари келтирилган.

Ушбу китобда ёритилган барча криптоалгоритмлар ва такомиллашган диаматрицалар алгебраси ва параметрли алгебраик структуралар республикамизда ахборот ва коммуникация тизимларининг ахборот хавфсизлиги муаммосини ҳал килишда, янги криптотизимлар ишлаб чиқишда ва криптография йўналишида илмий тадқиқотлар олиб боришда ҳамда ўқув муассасаларида криптография фанидан таълим беришда кенг қўлланилиши мумкин.

ISBN 978-9943-356-00-9

МУНДАРИЖА

СЎЗ БОШИ

Ахборот ва коммуникация технологияларининг (АКТ) жадал суръатлар билан ривожланиши ва Ўзбекистонни жаҳон глобал ахборот жамиятига кириб бориши ахборот хавфсизлигини таъминлаш йўналишида бир қатор вазифаларни бажаришни тақозо этади. АКТ тизимларига бўладиган хуружларнинг олдини олиш, ахборот хавфсизлигини таъминлаш — мамлакатни ички ва ташқи хавфлардан ҳимоялаш демакдир. Бу масалалар ҳал қилинмасдан, республикада АКТни кенг кўламда қўллаш қийинчиликларга олиб келиши мумкин.

Бутун жаҳонда ахборот хавфсизлигини таъминлашнинг илмий асосларидан бири — криптография фани тан олинган. Шуни ҳисобга олиб, Ўзбекистон Республикаси Президенти И.А. Каримов ушбу фанни ривожлантиришга катта эътибор бериб келмоқдалар. Республикада Ўзбекистон алоқа ва ахборотлаштириш агентлигининг Фан-техника ва маркетинг тадқиқотлари марказида биринчилардан бўлиб, криптография йўналиши бўйича илмий тадқиқотлар олиб боришга мўлжалланган бўлим ташкил этилди ва у ҳозирги кунда АКТ тизимларининг хавфсизлигини таъминлаш йўналишида фаол хизмат кўрсатиб келмоқда. Марказ олимларининг криптография соҳасида олиб борган тадқиқот натижалари ишлаб чиқилган бир қанча давлат стандартлари ва меъёрий ҳужжатлар сифатида намоён бўлди.

Ушбу китоб Ўзбекистон алоқа ва ахборотлаштириш агентлиги тизимида илмий изланиш олиб бораётган тадқиқотчи томонидан ёзилган бўлиб, унинг сўнгги йилларда олиб борган тадқиқотлари натижасини ўз ичига олади. Китоб криптография соҳасида ўзбек тилида чиқарилган илк очик нашр бўлиб, унда асосан криптографик тизимлар яратишга янгича ёндашувлар, янги алгебраик структуралар ёритилган. Илмий изланишларнинг натижалари нафақат республикамизда, балки дунё миқёсида ҳам криптография соҳасини ривожлантиришда катта аҳамият касб этиши мумкин.

Китобда келтирилган алгоритмлар ва алгебраик структуралар АКТ хавфсизлигини таъминлашда, илмий тадқиқотлар олиб боришда ҳамда ўқув муассасаларида криптография фанидан таълим беришда хизмат қилиши мумкин.

А. Арипов,
ЎзААА Бош директори, и.ф.н.

КИРИШ

Бутун жаҳонда ахборот ва телекоммуникация технологияларининг жадал суръатлар билан ривожланиши ҳамда республикамизнинг глобал ахборот жамиятига тобора катта қадамлар билан кириб бориши ахборот хавфсизлигини таъминлаш бўйича катор муҳим илмий тадқиқотлар олиб боришни тақозо этади. Ахборот хавфсизлигини таъминлашнинг илмий асоси бўлиб криптография фани тан олинган. Шу сабаб республикамизда ҳам сўнгги йилларда криптография йўналишига бўлган кизиқиш тобора ортиб бормоқда. Ушбу йўналишни ривожлантиришга давлатимиз томонидан ҳам катта аҳамият берилмоқда. Бунга кейинги йилларда қабул қилинган бир нечта қонун ва меъёрий ҳужжатлар, жумладан, «Электрон рақамли имзо», «Электрон ҳужжат айланиши» тўгрисидаги қонунлар, Президентимизнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари» тўғрисидаги қарори мисол бўлиши мумкин.

Ҳозирги кунга қадар ахборотни криптографик ҳимоя қилиш воситалари бутун дунёда ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири бўлиб хизмат қилиб келмоқда.

Шуни ҳисобга олиш керакки, хорижий давлатлар бошқа давлатларга криптографик ахборот-телекоммуникация воситаларини экспорт қилар эканлар, улар асосида амалга оширилган ахборот муҳофазаси тизимида етарли даражада бардошлиликка эга бўлмаган криптографик воситалар қатнашиши эҳтимоли йўқ эмас. Чунки, хорижга экспорт қилинадиган бундай воситалар миллий хавфсизлик органларининг текширувларидан ўтказилгандан сўнггина сотишга рухсат этилади. Бу эса, ўз навбатида, Ўзбекистон Республикасига кириб келаётган барча воситаларни ахборот хавфсизлиги талабларига мувофиқлигини текшириш, давлат аҳамиятига эга бўлган жойларда эса, фақатгина республикамизда ишлаб чиқарилган криптографик воситалардан фойдаланиш ва миллий тизимлар яратиш заруриятини туғдиради.

Криптографик воситаларни яратишда модуль арифметикасида матрицалар ва бутун сонлар алгебраларидан кенг фойдаланилади. Булар ҳозирги кунга қадар дунёга кенг тарқалган барча криптоалгоритмлар асосида ётади. Маълумки [1-8], шифр яратишда дастлабки маълумотларнинг биргина элементи ўзгариши натижасида шифрматнинг барча элементлари тамомила ўзгариши жуда муҳимдир. Аммо, бу мақсадда матрицалар алгебрасидан фойдаланилганда, ҳар шифрлаш босқичида шифр-матн матрицасининг фақат бир устун ёки сатр элементлари ўзгаради. Матрицавий алмаштиришлардан фойдаланишга асосланган шифрлар, масалан АҚШ стандарти AES [7, 9] да дастлабки маълумотлар блокининг байт сатҳидаги битта элементи ўзгарганда, биринчи босқичда аралаштириш *4* та элементнинг ўзгаришига олиб келади. Бу ҳар бир босқич учун шифралмаштириш криптобардошлилигининг пасайишига, натижада зарур криптобардошлиликни таъминлаш учун шифрлаш босқичларининг сонини кўпайтиришга ва шифрлаш тезлигининг пасайишига олиб келади. Шу боисдан, матрицалар алгебрасини криптографик криптобардошлилик нуқтаи назаридан такомиллаштириш ва улар асосида криптотизимлар яратиш усуллари ва алгоритмларини ишлаб чиқиш долзарб муаммолар қаторига киради.

Ушбу китобда криптография соҳасидаги етакчи давлатлар АҚШ, Россия ва Европа мамлакатларининг давлат стандартлари ва алгоритмлари билан бир қаторда, ҳозирги кунда энг кўп қўлланиладиган, энг ишончли деб тан олинган криптографик алгоритмларни яратишга асос бўлган умумий ёндашувлар, алгебраик структуралар ва функциялар баён этилган.

Китобда такомиллашган диаматрицалар алгебраси ва параметрли алгебраларни келтириб чиқариш, улар асосида янги криптоалгоритмлар яратиш ва мавжуд криптоалгоритмларни такомиллаштиришнинг умумий усуллари келтирилган. Маълумки, диаматрицалар алгебраси 1974 йилда Ўзбекистонда хизмат кўрсатган фан арбоби, т.ф.д., профессор П.Ф. Хасанов томонидан ишлаб чиқилган бўлиб, шу кунга қадар чизиқли электромагнит ва электр занжирлари ҳамда тизимлари анализи ва синтези масалаларини эффектив ечиш учун мўлжалланган

эди [10-13]. Бунинг сабаби, матрицалар алгебрасида тузиладиган чизиқли занжирнинг модели символли кўринишда диаматрицалар алгебрасида бирорта ҳам қўшимча ҳисоблашларсиз акс этишидадир. Диаматрицалар алгебрасини криптография йўналиши учун такомиллаштириш ва унинг асосида янги алгебраик структураларни яратиш ҳамда улардан фойдаланиш ҳозирги кунда мавжуд чет эл криптоалгоритмларидан кўра криптобардошлилиги юқори бўлган алгоритмлар яратиш имконини берди. Мисол учун, симметрик шифрлар яратишда матрицалар алгебраси ўрнига такомиллашган диаматрицалар алгебрасидан фойдаланиш ҳар босқич сўнггида шифрматн матрицасининг 1,5-1,75 баравар кўп элементларини ўзгаришига олиб келди.

Кейинги йилларда бир гуруҳ ўзбек олимлари томонидан олиб борилган изланишлар [14-31] шуни кўрсатдики, республикамизда криптографик алгоритмлар яратишда такомиллашган диаматрицалар алгебрасидан ва унинг асосида шакллантирилган бутун сонли ва матрицавий параметрли алгебрадан фойдаланиш кўпгина мавжуд муаммоларнинг ҳал этилишига ҳам хизмат қилади. Кўп ҳолларда мавжуд криптоалгоритмлар параметрли алгебра асосида яратилган алгоритмларнинг хусусий ҳоли бўлиб қолмоқда.

Ушбу китобда ёритилган барча криптоалгоритмлар ва такомиллашган диаматрицалар алгебраси ва параметрли алгебралар республикамизда ахборот ва коммуникация тизимларининг ахборот хавфсизлиги муаммосини ҳал қилишда, янги криптотизимлар ишлаб чиқишда ва криптография йўналишида илмий тадқиқотлар олиб боришда ҳамда ўқув муассасаларида криптография фанидан таълим беришда кенг қўлланилиши мумкин.

Китоб 206 бетда тақдим этилган бўлиб, 7 та бўлимдан, хулоса ва иловалар ҳамда фойдаланилган адабиётлар рўйхатидан иборат.

1-бўлимда шу кунга қадар дунёда кенг тарқалган ҳамда энг пухта деб тан олинган кўпгина симметрик ва носимметрик криптотизимлар, уларни яратишга асос бўлган алгебраик структуралар ва функциялар ёритиб берилган.

2-бўлимда муаллиф томонидан такомиллаштирилган диаматрицалар алгебраси, диаматрица-устунлар алгебраси, бутун сонли ва матрицавий параметрли алгебра, алгебраларнинг асосий амаллари ҳамда алгебраик амалларнинг хоссалари келтирилган. Криптография масалаларини ечиш учун мўлжалланган содда ва махсус тузилмали диаматрицалар устида бажариладиган асосий амалларни бажариш алгоритмлари ёритилган.

3-бўлимда диаматрица-устунлар алгебрасида, бутун сонли ва матрицавий параметрли алгебраларда дискрет даражага ошириш амалларини бажариш, бир томонлама бутун сонли ва матрицавий параметрли функцияларнинг хоссалари келтирилган.

4-бўлимда параметрли функция хоссаларига оид даража параметри муаммоси таърифлари, бутун сонли ва матрицавий даража параметри муаммоларига мос Диффи-Хэллман муаммолари баён этилган.

5-бўлимда симметрик криптотизимларни диаматрицалар алгебралари асосида яратиш усули, шифрлаш алгоритмининг асосий массивлари, диаматрицалар алгебралари амаллари асосида оддий ва функционал алмаштиришлар баён этилган. Шифрнинг псевдокоди ва алмаштиришлари келтирилган.

6-бўлимда диаматрица-устунлар алгебраси ва параметрли алгебра асосида носимметрик криптотизимлар яратиш усули, шифр яратишга Полиг-Хэллман, RSA, Тоҳир Ал Жамол усуллари, электрон рақамли имзо криптотизимини яратишга RSA ва умумий схема усуллари, махфий калит алмашув алгоритмини яратишга Диффи-Хэллман усулида ёндашувлар баён этилган. Олиб борилган тадқиқотлар асосида ишлаб чиқилган ҳимояланган электрон ҳужжат алмашиш тизими «Е-ҲУЖЖАТ» ҳақида қисқача ахборот келтирилган.

7-бўлимда параметрли функциядан фойдаланишга асосланган криптотизимлар криптобардошлилиги таҳлилининг мураккаблиги конуний ва ноконуний томонлар учун ҳар хиллиги, криптотаҳлилни амалга ошириш йўналишлари ва электрон рақамли имзо криптотизими криптобардошлилигининг баҳоси ёритилган.

Хулоса қисмида китоб бўлимлари бўйича асосий натижа ва хулосалар келтирилган.

Келтирилган иловалар иккита.

1-иловада такомиллаштирилган диаматрицавий шифр алмаштириши учун кириш массиви элементи ўзгаришига мос чиқиш элементларининг ўзгариш соҳалари келтирилган.

2-иловада муаллиф томонидан ишлаб чиқилган симметрик шифрлардан фойдаланиш учун маълумот алмашиш протоколлари ёритилган.

Ушбу китобнинг таҳририда ва уни босмага чиқаришда яқиндан ёрдам берган и.ф.н. А.Н. Арипов, т.ф.д., проф. С.С. Қосимов, т.ф.н. М.М. Маҳмудов, т.ф.д., проф. С.К. Ганиев, академик Ж.А. Абдуллаев, т.ф.д., проф. П.Ф. Хасанов, т.ф.д., проф. М.М. Мусаев, т.ф.д. проф., М.М. Каримов, т.ф.д., проф. М.М. Мухитдинов, т.ф.н., доцент Р.И. Исаев, т.ф.н., доцент Р.В. Қобулов, т.ф.н. О.П. Аҳмедова ҳамда дастурчилар Э.Э. Қиёмов, Р.Э. Қиёмовларга ўз миннатдорчилигимни билдираман.

1-БЎЛИМ

МАВЖУД КРИПТОТИЗИМЛАР ВА УЛАРНИ ЯРАТИШГА АСОС БЎЛГАН АЛГЕБРАИК СТРУКТУРАЛАР ВА ФУНКЦИЯЛАР

1.1 Симметрик ва носимметрик криптотизимлар

Криптографик криптотизимлар иккита синфга бўлинади: симметрик (махфий калитли, бир калитли) ва носимметрик (ошкора калитли, икки калитли) криптотизимлар. Ўз навбатида, симметрик криптотизимлар милоддан аввалги даврлардан маълум бўлиб, улар оқимли ва блокли шифр турларига бўлинади. Криптотизимларнинг ривожланиш тарихи [32-36] тўрт босқичга — дастлабки (XVI аср бошларигача), формал (XV аср охири XX аср бошлари), илмий (XX асрнинг 30-60-йиллари) ва компьютерли (замонавий) (XX асрнинг 70-йилларидан бошлаб) криптография даврларига бўлинади.

Симметрик криптотизимларнинг илмий назарияси яратилиши ва амалиёти ривожига илмий криптография асосчиси К. Шеннон [37] ва формал криптография намояндалари О. Керхгофф, Ч. Беббиж, У. Фридман, Г. Вернам, Э. Хеберн ва бошқалар катта ҳисса қўшган. Минг йиллар давомида криптография ҳарбий ва дипломатия алоқасини муҳофазалашда фойдаланиб келинган. Аммо ахборот асри бошланиши билан криптография хусусий секторда фойдаланиш учун ҳам зарур бўлиб қолди. Ҳозирги кунда пинҳона ахборотнинг (масалан, юридик ҳужжатлар, молиявий, кредит ставкалари тўғрисидаги ахборотлар, касаллик тарихи ва шу каби) талай қисми компьютерлараро алоқа линиялари орқали узатилмоқда. Жамият учун бундай ахборотнинг пинҳонийлиги ва асл ҳолда сақланиши заруратга айланган [38].

Носимметрик криптотизимлар бундан 32 йил муқаддам АҚШ олимлари У. Диффи ва М. Хэллман [39-44] томонидан кашф этилган бўлиб, улар катта сонли чекли тўпламларда бир томонлама функциялардан фойдаланишга асосланган. У. Диффи ва М. Хэллманнинг 1976 йилда босилиб чиққан "Криптоло-

гияда янги йўналишлар" мақоласида илгари сурилган "махфий калитни узатишни талаб этмайдиган амалий бардошли махфий тизимларни тузиш мумкин" деган фикри криптологияда носимметрик криптотизимларнинг юзага келиши ҳамда уларнинг ривожланиш давринининг бошланишига сабаб бўлди.

Носимметрик криптотизимлар назарияси ва амалиёти ривожига У. Диффи ва М. Хэллман билан бир қаторда Р. Райвест, А. Шамир, Л. Адлеман [44-52], Т. Жамол [53-54], К. Шнорр [55-57], В. Миллер [58], Н. Коблиц [59-61], А. Менезец [62-63], Б. Шнайер [1, 2, 64-66] катта ҳисса қўшган. Ҳозирги кунда криптографиянинг ривожланишига россиялик В. Матюхин [67], М. Молдовян, Н. Молдовян, Б. Изотов [3, 8, 68], А. Ростовцев [69-71] ҳамда ўзбекистонлик бир гуруҳ олимлар [23-26, 72-75, 100] ҳам муносиб ҳисса қўшмоқдалар.

Носимметрик криптотизимларнинг юзага келиши симметрик тизимларда ечилмай қолган махфий шифрлаш калитларини тарқатиш ва электрон рақамли имзо тизимларини яратиш ҳамда қатор замонавий масалаларни ечиш имкониятини берди.

Носимметрик криптотизимлар симметрик криптотизимларга нисбатан ўнлаб марта катта узунликдаги (*512, 1024, 2048, 4096* битли) калитлардан фойдаланади ва шу сабаб юзлаб марта секинроқ ишлайди. Носимметрик криптотизимларнинг математик асосида бир томонлама осон ҳисобланадиган функциялар (модуль бўйича дискрет даражага ошириш функцияси, эгри чизиқли эллиптик функция ва ш.к.) ётади. Носимметрик криптотизимлар ахборот хавфсизлигининг барча муаммоларини ечиб беришга қодир ҳисобланади.

Қуйида блокли шифрлар синфига мансуб бўлган маълумотларни шифрлаш алгоритмлари тўғрисида сўз боради.

1.2 Маълумотларни шифрлаш алгоритмлари

Шифрлаш — берилган (дастлабки) ахборотни шифрлаш калити ёрдамида бегона одам олиб тушунмайдиган шаклга, яъни шифрланган ахборотга айлантиришдир. Шифрни очиш эса шифрланган ахборотни уни (шифрлаш) очиш калити ёрдамида дастлабки ахборотга айлантиришдир. Шифрни бузиб очиш

деганда, шифрни очиш калитини билмаган ҳолда, шифрланган ахборотни дастлабки ахборотга айлантириш тушунилади. Шифрланадиган ахборот, умуман олганда матн, овоз ёзуви ва тасвир шаклида ёки аралаш шаклда берилиши мумкин. Амалиётда шифрланадиган ахборот асосан матн шаклида (иккилик, ўн олтилик саноқ тизимида) берилади ва у шифрматнга айлантирилади [38].

Ахборот узатиш ва сақлаш жараёнларининг рақамлаштирилиши узлукли (нутқ) ва узлуксиз (матн, факс, телекс, тасвир, анимация) ахборотни ҳимоя қилиш учун ягона алгоритмлардан фойдаланиш имконини беради. Бундан буён шифрланадиган ахборот матн шаклида берилган деб фараз қилинади.

Шифрлаш алгоритмларига қўйиладиган асосий талаблар қуйидагилардир [76, 77]:

— шифрланган ахборотни ўзгартириб қўйиш ёки шифрни бузиб очишга йўл қолдирмаслик;

— ахборот ҳимояси фақат калитнинг маълумлигига боғлиқ бўлиб, алгоритмнинг маълум ёки номаълумлигига боғлик бўлмаслик (О. Керхгофф қоидаси);

— дастлабки (шифрланадиган) ахборотни ёки калитни бироз ўзгартириш шифрланган матнни бутунлай ўзгартириб юбориши лозим (К. Шеннон тамойили, "ўпирилиш" ҳодисаси);

— калит қийматлари соҳаси шундай катта бўлиши керакки, унда калит қийматларини бир бошдан кўриб чиқиш асосида шифрни бузиб очиш имкони бўлмаслиги лозим;

— алгоритм иқтисодий жиҳатдан тежамли ва етарли тезкорликка эга бўлиши лозим;

— шифрматнни бузиб очишга кетадиган сарф-харажатлар ахборот баҳосидан юқори бўлиши лозим.

Криптографик тизим ёки қисқача криптотизим, шифрлаш ҳамда шифрни очиш алгоритмлари, бу алгоритмларда ишлатиладиган калитлар, шифрланадиган ҳамда шифрланган матнлар ва буларни ўзаро мослашиш қоидаларини ўзида мужассамлаштирган протоколдан иборат мажмуавий тизимдир [1, 7].

Криптотизимдан фойдаланишда, матн муаллифи шифрлаш алгоритми ва шифрлаш калити воситасида, аввало дастлаб-

ки матнни шифрланган матнга ўгиради. Матн муаллифи уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқариш тизимига ҳожат бўлмайди), уни сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса, сақлаб қўйилган ахборотнинг бутунлиги таъминланган бўлади. Акс ҳолда ахборот бутунлиги бузилган бўлиб чиқади.

Агар шифрланган матн уни яратган муаллифдан ўзга қонуний фойдаланувчига (олувчига) мўлжалланган бўлса, у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан, унга аввалдан маълум бўлган шифрни очиш калити ва алгоритми асосида, дастлабки матнга айлантирилади.

Криптотизимда ахборотни шифрлаш ва унинг шифрини очишда ишлатиладиган калитларнинг турига кўра улар бир калитли (симметрик, махфий калитли) ва икки калитли (носимметрик, ошкора калитли) тизимларга ажратилган. Одатда барча криптотизимларда шифрлаш алгоритми шифрни очиш алгоритми билан айнан ёки бироз фарқли бўлади. Криптотизим "қулфининг" бардошлилиги, алгоритм маълум бўлган ҳолда калитнинг муҳофаза хоссаларига, асосан, калит узунлиги (битлар сони)нинг катталигига боғлик деб қабул қилинган.

Кейинги бандда блокли симметрик шифрлар синфига мансуб бўлган маълумотларни шифрлашнинг машҳур алгоритмлари, уларнинг архитектураси ва уларни яратишга асос бўлган алгебраик амаллар ҳақида сўз боради.

1.3 Симметрик шифрлар

Криптографлар орасида машҳур бўлган маълумотларни шифрлаш алгоритмлари гуруҳига АҚШ давлат стандартлари — DES (Data Encryption Standard) [1, 78], AES (Advanced Encryption Standard) [9], Россия Федерацияси давлат стандарти ГОСТ-28147-89 [79] ҳамда IDEA (International Encryption Algorithm) [1, 7], FEAL [1, 7] киради.

DES IBM фирмасининг бутун бир гуруҳ криптографлари томонидан ишлаб чиқилган [4] маълумотларни шифрлаш стандарти Миллий Стандартлар Бюроси томонидан 1976 йилнинг

23 ноябрида АҚШ давлат стандарти сифатида қабул қилинган ва у 1977 йилнинг июлидан 2000 йилнинг октябрь ойига қадар рақамли маълумотларни шифрлаш учун стандарт бўлиб хизмат қилган. Ҳозирги вақтда у фақат назарий аҳамиятга эга.

DES занжирсимон тузилмали мувозанатланган Фейстал тармоғи архитектурасига эга. Алгоритмда дастлабки матн *X*, шифрматн *У* блоклари ва калит *Z* — иккилик саноқ тизимидаги кетма-кетликлар бўлиб, бу ерда мос равишда *X=64, У=64* ва *K=56* бит узунликка эга. Умумий ҳолда *X* барча 2^{64} та қийматни қабул қилиши мумкин. *X=У=64* бўлгани учун DES жуда катта $2^{64}=10^{19}$ символли алифбодаги ўрнига қўйишдан фойдаланилади.

Мутахассисларнинг фикрига кўра, бу стандарт ёйиш ва аралаштиришга асосланган, энг яхши криптоалгоритмлардан биридир. Шифрлаш алгоритмида шифрматннинг ҳар бир бити дастлабки матн ва калит барча битларининг функцияси бўлади. Стандартда ўрнига қўйиш, ўрин алмаштириш ва *2* модуль бўйича қўшиш амалларини комбинациясидан фойдаланилади.

DESда дастлабки матнни шифрматнга ўгириш тартиботи кириш блоки устида бошланғич ва чиқишдан олдин якуний ўрин алмаштиришлардан, кириш блокини чап ва ўнг қисмларга ажратиб, улар устида *16* та кетма-кет келадиган босқич (раунд)ларни амалга оширишдан иборат. Ҳар бир босқич чап ва ўнг қисмларнинг ўрнини алмаштиришлар, ўрнига қўйишлар, кенгайтмали ўрин алмаштиришлар каби амалларни ўз ичига олади.

Чап қисм L_i ва ўнг қисм R_i (1.1) функция *f* орқали босқич калити K_i билан (1.2) ифода бўйича боғланган:

$$L_i=R_{i-1}, \qquad (1.1)$$

$$R_i=L_{i-1}\oplus f(R_{i-1}, K_i). \qquad (1.2)$$

Ҳар бир босқич калити *48* бит бўлиб, у *56* битли калитни босқичга боғлиқ ҳолда, бир ёки икки битга суриш орқали зичланмали ўрин алмаштиришлар натижасида генерацияланади. Бу тасодифий танлаш конуниятига бўйсунади. DES алгоритмининг ночизиқлилиги *S*-блоклар туфайли таъминланади. DESда *8* та ошкора *S*-блок мавжуд бўлиб, уларнинг ҳар бири *0* дан *15*

гача бўлган бутун сонлардан таркиб топган ўрнига қўйиш жадвали — *4x16* тартибли матрицани акс эттирувчи мувозанатланган Фейстал тармоғининг ўрнига қўйиш тугунларидир.

Шифрматнни дастлабки матнга ўгириш ҳам худди дастлабки матнни шифрматнга ўгириш каби бажарилади, фақат бунда босқич калитларини генерациялаш йўналиши ўзгаради.

ГОСТ-28147-89 — собиқ Совет Иттифоқида ишлаб чиқилган DES каби мувозанатланган Фейстал тармоги архитектурали, *64* бит блокли ва калит узунлиги *256* бит бўлган криптографик ўзгартириш алгоритмидир. Алгоритм босқичлари сони *32* га тенг бўлсада, у DESга нисбатан тезкордир.

Дастлабки матнни шифрматнга ўгириш жараёнида, DESдаги каби матн *L*-чап қисмга ва *R*-ўнг қисмга бўлинади. *i*-босқичда K_i қисмкалитдан фойдаланилади ва DESдаги каби (1.1) ва (1.2) амаллар бажарилади.

Аввал ўнг қисм *i*-калит билан 2^{32} модуль бўйича қўшилади. Натижа *4* битли саккизта бўлакка бўлинади, уларнинг ҳар бири эса ўзининг *S*-блоки киришига тушади. ГОСТ умумий ҳажми *512* бит бўлган саккизта *S*-блокдан фойдаланади, уларнинг ҳар бири *0* дан *15* гача бўлган бутун сонлардан таркиб топган ўрнига қўйиш жадвали — *8x16* тартибли матрицани акс эттирувчи алмаштириш тугунларидир. *S*-блоклар махфий сақланади.

Барча *8* та *S*-блокларнинг чиқиши битта *32* битли сўзга бирлаштирилади, сўнгра бутун сўз даврий равишда чапга *11* битга сурилади. Ва ниҳоят, натижа *XOR* амали ёрдамида чап қисм билан бирлаштирилиб, янги ўнг қисм ҳосил қилинади. Бунда аввалги ўнг қисм янги чап қисм бўлади. Бу амаллар *32* босқич давомида даврий равишда бажарилади.

Қисмкалитларни генерация қилиш жараёни DESга нисбатан содда. Бунинг учун *256*-битли калит *8* та *32* битли блокка ажратилади: $k_1, k_2, \ldots k_8$. Ҳар бир босқичда унга мос қисмкалит ишлатилади.

Шифрматнни дастлабки матнга ўгириш ҳам, худди дастлабки матнни шифрматнга ўгириш каби бажарилади, фақат бунда калитлар кетма-кетлиги ўзгартирилади.

ГОСТ-28147-89да DES, AESга хос электрон код китоби маромига ўхшаш оддий алмаштириш мароми, DES, AESга хос

маромлардан бироз фарқли бўлган гаммалаштириш, тескари боғланишли гаммалаштириш маромлари ва улардан принципиал фарқ қилувчи имитоқистирма ишлаб бериш маромидан фойдаланади. Имитоқистирма ишлаб бериш мароми шифрматнларни узатишда ва сақлашда уни тасодифий ва қасддан ўзгартириб қўйишнинг олдини олишга хизмат қилади. Гаммалаш мароми гамма блокини битлаб қўшиш орқали шифрматн блокини шакллантиришдан иборат бўлиб, унда фойдаланиладиган ҳар бир *64* битли гамма блоклари алгоритмик реккурент сонлар кетма-кетлиги генератори (РГПЧ) ёрдамида ҳосил қилинади. Бунда ҳар бир кириш блокини оддий алмаштириш маромидан фойдаланилади. Шифрматнни дастлабки матнга ўгиришда томонлараро РГПЧ лар ўзаро мос ҳолда инициализацияланиши зарурлиги шифрматн билан бирга *64* битли синхрожўнатма сигналини ҳам қўшиб жўнатишни тақозо этади. Бу маълум қийинчиликлар туғдирсада, ўзини оқлайди.

ГОСТ-28147-89 *S*-блокларни генерация қилиш усулларини белгиламайди, фақат *S*-блоклар қандай тақдим этилиши керак дейилади, холос. Бу эса, ўз навбатида, бир алгоритм орқали ҳар хил криптобардошлиликка эга бўлган криптотизимларни ярата олиш яхши *S*-блоклар ва ёмон *S*-блоклар ҳосил қилишга ҳам боғлиқлигини кўрсатади. ГОСТ-28147-89да *256* битли калитдан, махфий *S*-блоклардан ва РГПЧ дан фойдаланилиши унинг DESга нисбатан анча юқори криптобардошлилигини таъминлайди. Бу кунгача у энг эффектив ҳисобланган дифференциал ва чизиқли криптотаҳлил усулларига нисбатан етарли даражада криптобардошли саналадиган алгоритмлардан биридир.

ГОСТ-28147-89дан фарқли ўлароқ, жуда кўп соҳаларда фойдаланиб келинган DES 90-йиллар охирида иккита асосий сабабга кўра кенг қўллаш учун яроқсиз бўлиб қолди.

Биринчидан, DESда калит узунлиги *56* бит бўлганлиги ахборот технологияларининг 2000 йилга келиб ривожланган даражаси учун жуда қиска эди.

Иккинчидан, DES алгоритми яратилганда, уни қурилма шаклида ишлаб чиқариш кўзда тутилганлиги сабабли, *8* битли микропроцессор учун мўлжалланган амаллар (масалан,

машина сўзидаги битларнинг ўрнини маълум схема ёрдамида алмаштириш) катта вақт талаб этарди.

Шунинг учун, 1997 йилда Америкaнинг стандартлаш институти NIST (National Institute of Standards & Technology) янги симметрик криптоалгоритм — AES (Advanced Encryption Standard) ишлаб чиқиш учун бутун дунёдаги илгор криптология марказлари ўртасида танлов эълон қилди. Бу мусобақанинг голиби кейинги 10—20 йил учун деярли умумжаҳон криптостандарти бўлиши мўлжалланган эди.

Янги AES стандартига даъвогар бўлган криптоалгоритмларга қуйидаги талаблар қўйилди [7]:

— алгоритм симметрик бўлиши керак;

— алгоритм блокли шифр бўлиши керак;

— алгоритм блокининг узунлиги *128* бит бўлиб, *128*, *192* ва *256* битли уч хил узунликдаги калитларни қўллаш мумкин бўлиши керак.

Шунингдек, криптоалгоритм ишлаб чикарувчиларга қўшимча йўриқлар ҳам берилди:

— ҳам қурилмада (микрочипларда), ҳам дастур сифатида (шахсий компьютерларда ва серверларда) осон қўлланиладиган амаллардан фойдаланиш;

— *32* разрядли процессорларга мўлжаллаш;

— шифр структурасини заруриятсиз кийинлаштирмаслик, бунда барча қизиқувчи томонлар мустақил равишда алгоритмнинг криптотаҳлилини ўтказишлари ва унда ҳеч бир ҳужжатда кўрсатилмаган имкониятларнинг мавжуд эмаслигига ишонч ҳосил қилишлари кўзда тутилган.

Ташкилот қўмитаси томонидан турли мамлакатлардан тушган 15 та ариза икки йил давомида ҳар томонлама ўрганиб чиқилгандан сўнг, 2000 йилнинг 2 октябрида NIST ғолибни маълум қилди. Мусобака голиби деб бельгиялик икки мутахассис Ж. Деймен ва В. Рижмен томонидан ишлаб чиқилган квадрат архитектурали Rijndael алгоритми эълон килинди ва шу вақтдан бошлаб бу алгоритмга қўйилган барча патент чекловлар бекор қилинди.

AES алгоритмида ҳар бир кириш блоки, ўрнатилган узунликка мос равишда, икки ўлчамли *4*x*4*, *4*x*6* ёки *4*x*8* массиви би-

лан тақдим этилади. Шифрлаш босқичлари давомида алмаштиришлар алоҳида байтлар устида бажарилади. AESда кириш блоки ва чиқиш блоки узунлиги *128* бит (Rijndael алгоритмида *128*, *192* ёки *256* бит), шифрлаш калитининг узунлиги *128*, *192* ёки *256* бит бўлади.

Шифрлашда қўлланиладиган барча алмаштиришлар ёйилиш ва тарқалиш тамойилларини амалга оширишга қаратилган. Стандартда, блок ва калитнинг узунлигига боғлиқ равишда, босқичлар сони *10* тадан *14* тагача белгилаб қўйилган.

Шифрлаш тартиботи боскич калитларини генерациялаш тартиботини ҳам, босқичлар сонига мос узунликдаги шифрматнга ўгириш (дастлабки матнга ўгириш) учун босқич калитларини юклашни ҳам ўз ичига олади.

Дастлабки матнни шифрматнга ўгириш жараёнида ҳар бир босқичда қуйидаги амаллар кетма-кет бажарилади:

BS: ҳар бир байт устида жадвалли ўрнига қўйиш (байтли алмаштириш) (ночизиқли амал);

SR: қатор элементларини турли силжиш қийматларига суриш (чизиқли амал);

MC: полиномли модуль бўйича *C* матрицага кўпайтириш (чизиқли амал);

AK: XOR, калитни битлаб қўшиш амали (чизиқли амал).

Сўнгги босқичнинг тузилиши ундан олдинги барча босқичлардан *MC* амали иштирок этмаслиги билан фарқланади. Шундай қилиб, шифрлаш алгоритмининг бажарилиши қуйидаги кўринишга эга:

AK, {*BS*, *SR*, *MC*, *AK*} *(*R-1* марта), *BS*, *SR*, *AK*.

Шифрматнни дастлабки матнга ўгириш амалларни инверсия (тескари) тарзида бажариш орқали амалга оширилади:

$BS_{тес}$: ҳар бир байт устида тескари жадвалли ўрнига қўйиш (байтли алмаштириш);

$SR_{тес}$: қатор элементларини тескари йўналишда турли силжиш қийматларига суриш;

$MC_{тес}$: полиномли модуль бўйича *D* матрицага кўпайтириш, бу ерда $D=C^{-1}$, $C \times D=1$.

$AK_{тес}$: XOR, калитни битлаб қўшиш амали ўз-ўзига тескари, бунда фақат калит элементларининг ишлатилиш тартиби ўзгаради, холос.

Шифрни бутунлай очиш қуйидаги кўринишга эга бўлади:

$AK_{тес}$, $SR_{тес}$, $BS_{тес}$, {$AK_{тес}$, $MC_{тес}$, $SR_{тес}$, $BS_{тес}$}*(*R-1* марта), $AK_{тес}$.

Ҳозирги кунгача AES юқори криптобардошлиликка эга бўлган шифрлар қаторига киради.

IDEA — яна бир *64* битли, блок шифрли алгоритм бўлиб, унинг калит узунлиги *128* битга тенг. IDEA шифрининг биринчи варианти К. Лай ва Д. Масси томонидан *1990* йилда таклиф этилган. У тезлиги бўйича DES алгоритмидан қолишмайди, криптотаҳлилга бардошлилиги жиҳатидан эса ундан ҳам устун.

IDEA алгоритми билан дастлабки матнни шифрматнга ўгириш шифрматнни дастлабки матнга ўгиришда ҳам ягона алгоритмдан фойдаланилади.

IDEA алгоритмида ҳам бошқа блокли шифрлаш алгоритмларидаги каби аралаштириш ва ёйиш тамойиллари етарли даражада амалга оширилган. Унинг асосини "турли алгебраик гуруҳларнинг амалларини бирлаштириш" фалсафаси ташкил этади. Унда учта алгебраик гуруҳ аралаштирилган ва уларнинг барчаси ҳам қурилма, ҳам дастур кўринишида осон амалга оширилади.

Бу гуруҳлар:

— *XOR*,

— 2^{16} модуль бўйича қўшиш,

— $2^{16}+1$ модуль бўйича кўпайтириш (Бу амални IDEA алгоритмининг блоки сифатида қараш мумкин).

64 битли блок *16* битли *4* та қисмблокка бўлинади: X_1, X_2, X_3 ва X_4. Бу *4* та қисмблоклар алгоритмнинг биринчи босқичига кирувчи маълумотлар бўлади. Ҳаммаси бўлиб алгоритм *8* та босқичдан иборат. Ҳар бир босқичда *4* та қисмблок ўзаро бир-бири билан ва *16* битли қисмкалитлар билан *XOR* амали, қўшиш ва айириш амаллари ёрдамида муносабатда бўлади. Босқичлар орасида иккинчи ва учинчи қисмблоклар ўрин алмашинади. Ва ниҳоят, охирги алмаштиришда *4* та қисмблок *4* та қисмкалит билан бирлаштирилади.

Саккизинчи босқичдан кейин охирги алмаштириш қуйидаги тартибда бажарилади:

X_1 ва биринчи қисмкалит кўпайтирилади;

X_2 ва иккинчи қисмкалит қўшилади;

X_3 ва учинчи қисмқалит қўшилади;

X_4 ва тўртинчи қисмкалит кўпайтирилади.

Ва ниҳоят, *4* та қисмблоклар яна бирлаштирилиб, шифрматн ҳосил қилинади.

Қисмкалит яратиш ҳам унчалик қийин эмас. Аввал *128* битли калит *8* та *16* битли қисмкалитларга бўлинади (*6* таси биринчи босқич учун, *2* таси эса иккинчи босқич учун). Сўнгра калит чап тарафга *25* битга циклик сурилади ва яна *8* та қисмкалитга бўлинади. Биринчи тўрттаси иккинчи босқичда, қолган тўрттаси эса учинчи босқичда ишлатилади. Кейинги *8* та қисмкалитларни ҳосил қилиш учун калит яна чап тарафга *25* битга циклик сурилади ва ҳ.к.

Шифрни очиш амали ҳам худди шифрлаш амали каби бажарилади, бунда фақат қисм калитлар бироз ўзгартирилади.

FEAL алгоритми япон мутахассислари А.Шимузу ва Ш.Миягучи томонидан таклиф этилган бўлиб, унда кириш ва чиқишда *64* битли блоклардан ва *64* битли калитдан фойдаланилади. Унинг мақсади DESга нисбатан кучли алгоритм яратишдан иборат бўлган, лекин пировардида бу алгоритм бошланғич максаддан узоқлашиб кетган.

Дастлабки матнни шифрматнга ўгириш жараёнида аввал кириш блоки ва *64* битли калит устида *XOR* амали бажарилади. Сўнгра кириш блоки ўнг ва чап қисмларга ажратилади. Чап ва ўнг қисмларни *XOR* амали ёрдамида бирлаштириб янги ўнг қисм ҳосил қилинади. Чап ва янги ўнг қисм босқичларни ўтиб чиқади. Ҳар бир босқичда ўнг қисм *f* функцияси ёрдамида калитнинг *16* бити билан ва чап қисм *XOR* амали ёрдамида янги ўнг қисм ҳосил қилади. Бошланғич ўнг қисм (босқич бошида) янги чап қисм бўлади.

f функция киришнинг *32* битини ва калитнинг *16* битини олади ва уларни бирга аралаштиради. Аввал кириш блоки *8* битли қисмларга бўлинади, кейин *XOR* амали ёрдамида бирлаштирилади ва бир-бирини алмаштиради.

Худди шу алгоритм шифрматнни дастлабки матнга ўгириш учун ҳам ишлатилган. Бунда ягона фарқ шундаки, шифрматнни дастлабки матнга ўгиришда калит қисмларидан фойдаланиш тартиби тескарисига ўзгаради.

FEAL алгоритмининг муаллифлари томонидан унинг босқичлар сони ўзгарувчан (8 тадан ортиқ) бўлган модификациялари ишлаб чиқилган, аммо босқичлар сони 8, 16 бўлганда ҳам, улар дифференциал ва чизиқли криптотаҳлилга нисбатан етарли криптобардошлиликни таъминлай олмаганликлари маълум [1, 2]. FEAL алгоритми асосан криптотаҳлилчилар орасида машҳур, чунки кимда-ким янги криптотаҳлил усулини яратса, уни аввало FEAL алгоритми учун синаб кўриши одат тусига кирган.

Юқорида баён этилган ГОСТ-28147-89дан бошқа барча алгоритмларда маълумотларни шифрлашда электрон код китоби (ECB), шифр блокларнинг илашиши (CBC), чиқиш орқали тескари боғланиш (OFB), шифр матн орқали тескари боғланиш (тескари боғланишли гаммалаштириш) (CFB), саноқчи (CTR) каби *5* хил иш маромини қўллаш мумкин. Табиийки, ҳар бир иш мароминиг ўзига хос афзаллиги ва камчилиги бўлади. Масалан, калитларни шифрлашда электрон код китоби иш маромини, алоҳида белгилар учун шифрматн орқали тескари боғланиш иш маромини, алоқа тизимида (одатда, бирор шифрматнни такрор узатиш имконияти бўлмаганда) чиқиш орқали тескари боғланиш иш маромини қўллаш қулай ҳисобланади.

Электрон код китобидан бошқа маромлар, одатда, ҳар сеансда тасодифий танланадиган инициализация вектори (синхройўлланма)дан фойдаланиш туфайли шифрматн блокларини тасодифийлаштирилиши (рандомизация) натижасида шифр криптобардошлилигини оширишга имконият яратади.

DES, ГОСТ, AES, IDEA ва FEAL алгоритмларининг қиёсий кўрсаткичлари 1.1-жадвалда келтирилган.

Шифрлаш калитининг узунлиги, DES ва FEAL алгоритмларида энг қисқа (*56*, *64* бит), қолган алгоритмларда эса *128* битдан *256* битгача эканлиги келтирилган жадвалдан кўриниб турибди. Шифрланадиган блок узунлиги фақат AES учун *128* битга тенг, қолган алгоритмларда эса *64* битни ташкил этади. Шифр архитектураси фақат AES да квадрат шаклида бўлиб, қолган алгоритмларда тармоқ тузилмасига эгадир. Босқичлар сони IDEA учун минимал бўлиб, ГОСТ учун энг катта қийматга, қолган алгоритмлар учун оралиқ қийматларга эга.

1.1-жадвал

DES, ГОСТ, AES, IDEA ва FEAL алгоритмларининг қиёсий кўрсаткичлари

Кўрсаткич	DES	ГОСТ	AES	IDEA	FEAL
Блок узунлиги, бит	*64*	*64*	*128*	*64*	*64*
Шифрлаш калити узунлиги, бит	*56*	*256(S-блоклар махфий)*	*128, 192, 256*	*128*	*64*
Архитектура	*мувозанатланган Фейстал тармоги*	*мувозанатланган Фейстал тармоги*	*Квадрат*	*Занжирсимон тармоқ*	*мувозанатланган Фейстал тармоги*
Раундлар сони	*16*	*32*	*10, 12, 14*	*8*	*>16*
Раунд калити узунлиги, бит	*48*	*32*	*128*	*96*	*16*
Раунд калити тартиботи	*Бироз мураккаб*	*Содда*	*Мураккаб*	*Содда*	*Бироз мураккаб*
Раунд тузилмаси	*Содда*	*Содда*	*Нисбатан мураккаб*	*Содда*	*Содда*
Фойдаланадиган амаллар	*XOR*, ўрнига қўйиш, жой алмаштириш, кенгайтмали жой алмаштириш, зичламали жой алмаштириш,суриш ($GF(2^4)$, $GF(2)$)	*XOR*, қўшиш, ўрнига қўйиш, жой алмаштириш, суриш ($GF(2^{32})$, $GF(2^{32}-1)$, $GF(2)$)	*XOR*, ўрнига қўйиш (байт алмаштириш), полиномли модуль бўйича матрицавий кўпайтириш, суриш ($GF(2^8)$, $GF(2^8+1)$, $GF(2)$)	*XOR*, қўшиш, айириш, жой алмаштириш, суриш ($GF(2^{16})$, $GF(2^{16}+1)$, $GF(2)$)	*XOR*, қўшиш, ўрнига қўйиш, жой алмаштириш, суриш ($GF(2^8)$, $GF(2)$)
Тўғри ва тескари ўзгартиришлар эквивалентлиги	*Субкалит элементларининг тартиби аниқлигида*	*Субкалит элементларининг тартиби аниқлигида*	*Калит элементлари вектори, ўрин алмаштириш жадвали ва алгоритм доимийлари аниқлигида*	*Субкалитлар тескариланиш ва бироз ўзгартирилиши аниқлигида*	*Субкалит элементларининг тартиби аниқлигида*
Маромлар	электрон код китоби; шифрматн орқали тескари боғланиш; шифр блокларнинг илашиши; чиқиш орқали тескари боғланиш; саноқчи	оддий алмаштириш; гаммалаштириш; тескари боғланишли гаммалаштириш; имитокистирма ишлаб бериш	электрон код китоби; шифрматн орқали тескари боғланиш; шифр блокларнинг илашиши; чиқиш орқали тескари боғланиш; саноқчи	электрон код китоби; шифрматн орқали тескари боғланиш; шифр блокларнинг илашиши; чиқиш орқали тескари боғланиш; саноқчи	электрон код китоби; шифрматн орқали тескари боғланиш; шифр блокларнинг илашиши; чиқиш орқали тескари боғланиш; саноқчи

Барча шифрларда фойдаланилган амаллар тўплами модуль арифметикасида бажарилган бўлиб, суриш, иккилик модулда битлаб қўшиш ва ўрнига қўйиш (ночизиқли *S*-блок) амалларидан фойдаланиш уларнинг барчасига хос. Келтирилган алгоритмлар бир-биридан модуль қиймати ва тури билан фарқланади. Фақат AESда полиномли модулдан фойдаланилса, қолган алгоритмларда туб ва/ёки мураккаб модуль бўйича қўшиш ва кўпайтириш амалларидан фойдаланилади. IDEAда кўпайтириш амали ночизиқли *S*-блок вазифасини ўтайди.

Машҳур симметрик шифрлар ҳақида юқорида келтирилган маълумотларни реал вақт масштабида фойдаланишга энг қулай бўлган Интернет саҳифаларида "олтин криптография" [80] номи остида келтирилган янги симметрик шифр билан тўлдириш лозим топилди. Мазкур шифрлаш усули Тагонрог радиотехника университети (Россия) фахрий профессори А.П. Стахов томонидан таклиф этилган бўлиб, "олтин матрица" деб номланган *2x2* тартибли қуйида келтирилган матрицалардан фойдаланишга асосланади.

$$Q(2x_i) = \begin{vmatrix} cF_s(2x_i+1) & sF_s(2x_i) \\ sF_s(2x_i) & cF_s(2x_i-1) \end{vmatrix}$$

$$Q(-2x_i) = \begin{vmatrix} cF_s(2x_i-1) & -sF_s(2x_i) \\ -sF_s(2x_i) & cF_s(2x_i+1) \end{vmatrix}$$

"Олтин матрица" элементлари ҳақиқий сонлар тўпламининг элементи x_i нинг гиперболик синус ва косинуслари бўлиб, бу матрицаларнинг матрицавий кўпайтмаси бирлик матрицасига тенг, ихтиёрий x_i учун ҳар бирининг детерминанти бирга тенг. Дастлабки матн *i*-блокини шифрлашда $Q(2x_i)$ матрицадан, шифрматн *i*-блокини очишда $Q(-2x_i)$ матрицадан фойдаланилади.

Шифрлаш алгоритми (ёки шифратор-дешифратор курилмаси)нинг кириш ва чиқишида *тўрт элементли* матрицавий блоклардан ва ҳар бир *i*-блокни *икки қисмли* калит (K_i, x_i) билан шифрлашдан фойдаланилади. Унда раундлар сони битта,

юқори криптобардошлилик талаб қилинганда эса, бир нечта бўлиши мумкин.

Дастлабки матннинг ҳар бир *i*-блоки элементлар тўртлиги ($a_{i1}\,a_{i2}\,a_{i3}\,a_{i4}$) асосида шаклланган 2х2 тартибли қуйидаги матрица шаклида берилади.

$$M_i = \begin{vmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{vmatrix}$$

Шифратор-дешифратордан бир раундли маромда фойдаланиш жараёнлари қуйида баён этилган.

Дастлабки матнни шифрматнга ўгиришнинг бир раундли жараёнида ҳар бир блок устида бор-йўғи учта бир хил ўзгартиришлар кетма-кетлиги бажарилади:

1) $M_i \Rightarrow B_i$: ҳар бир элемент a_{ik} ўрнига, a_{iksj} қўйиш, бу ерда $k \in \{1, 2, 3, 4\}$; $s, j \in \{1, 2\}$;

$M_i \Rightarrow B_i$ ни амалга ошириш $4!=24$ усулда бажарилиши мумкинлигини эътиборга олиб, аввало *икки қисмли* калит (K_r, x_i) биринчи компонентаси K_i {1, 2, 3,... 24} тўпламдан танланади; бу ерда тўплам элементи ўрнига қўйиш усулининг тартиб рақами. Натижада K_i га мос қуйидаги B_i матрица шаклланади.

$$B_i = \begin{vmatrix} a_{i\,4\,11} & a_{i\,1\,12} \\ a_{i\,3\,21} & a_{i\,2\,22} \end{vmatrix}$$

2) $Q(2x_i)$ элементларини ҳисоблаш ва $Q(2x_i)$ ни шакллантириш;

буни амалга ошириш $Q(2x_i)$ нинг учта элементини ҳисоблаш натижасида бажарилади:

$$Q(2x_i) = \begin{vmatrix} (G^{2xi+1}+G^{-(2xi+1)})/2 & (G^{2xi}- G^{-2xi})/2 \\ (G^{2xi} - G^{-2xi})/2 & (G^{2xi-1}+G^{-(2xi-1)})/2 \end{vmatrix}$$

Бу ерда $G=(1+\sqrt{5})/2$.

3) $SH_i = B_i \times Q(2x_i)$, яъни шифрматн SH_i ни шакллантириш;

буни амалга ошириш матрицавий кўпайтма $B_i x Q(2x_i)$ ни ҳисоблашдан иборат.

SH_i канал орқали узатилади ва шифратор навбатдаги $i+1$ блокини шифрлашга ўтади ва ҳ.к. Бунда ҳар бир янги блок учун шифрлаш калити (K_i, x_i) янгиланади. Агар дастлабки матн n блокдан ташкил бўлган бўлса, шифрлаш калити $K=(K_1, x_1; K_2, x_2; ; ; ; K_n, x_n)$ кўринишини олади ва у томонлараро очиқ калитли махфий калитларни алмашиш алгоритми (Диффи-Хэллман ёки Ал Жамол усули) асосида ёки ҳимояланган алоқа канали орқали амалга оширилиши мумкин.

Шифрматнни дастлабки матнга ўгиришнинг бир раундли маромида ҳам ҳар бир блок устида бор-йўғи учта бир хил ўзгартиришлар кетма-кетлиги бажарилади:

1) $Q(-2x_i)$ элементларини ҳисоблаш ва $Q(-2x_i)$ни шакллантириш;

буни амалга ошириш $Q(-2x_i)$нинг учта элементини ҳисоблаш натижасида бажарилади:

$$Q(-2x_i) = \begin{vmatrix} (G^{2xi-1}+G^{-(2xi-1)})/2 & -(G^{2xi}-G^{-2xi})/2 \\ -(G^{2xi}-G^{-2xi})/2 & (G^{2xi+1}+G^{-(2xi+1)})/2 \end{vmatrix}$$

Бу ерда $G=(1+\sqrt{5})/2$.

2) $B_i = SH_i \times Q(-2x_i)$, яъни B_i ни шакллантириш;

буни амалга ошириш матрицавий кўпайтма $SH_i \times Q(-2x_i)$ни ҳисоблашдан иборат.

3) $B_i \Rightarrow M_i$: ҳар бир элемент a_{iksj} ўрнига a_{ik} қўйиш, бу ерда $k \in \{1, 2, 3, 4\}$; $s, j \in \{1, 2\}$;

$B_i \Rightarrow M_i$ ни амалга ошириш *икки қисмли* калит (K_i, x_i) биринчи компонентаси K_i асосида бажарилади. Натижада K_i^{-1} га мос

$$M_i = \begin{vmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{vmatrix}$$

тикланади. Бу ерда $K_i^{-1} K_i$ га тескари йўналишда бажариладиган мослик.

Агар дастлабки матнни шифрматнга ўгиришнинг $m>1$ раундли жараёнидан фойдаланилса, унда ҳар бир блок устида биринчи раундда 1), 2) ва 3) ўзгартиришлардан, ундан ке-

йинги (*m-1*) раунд давомида шифрлаш ўзгартиришларининг 2) ва 3) ўзгартиришларидан, шифрни очишда эса (*m-1*) раунд давомида 1) ва 2) ўзгартиришлардан, *m*-раундда 1), 2) ва 3) ўзгартиришлардан фойдаланилади. Шунга кўра шифрлаш калити $K = (K_1, x_{11}, \ldots x_{1m}; K_2, x_{21}, \ldots x_{2m}; ; ; ; K_n, x_{n1}, \ldots x_{nm})$ кўринишини олади.

Келтирилган симметрик шифрнинг афзалликларига қуйидагилар киради:

— алгоритм жуда соддалиги туфайли юқори тезкорлик билан шифрлашга эришилади, бу айниқса реал вақт масштабида ишлайдиган тизимлар (масалан, телефонда сўзлашувлар, мультимедиа, телевизион кўрсатувлар ва ҳ.к.) учун муҳимдир;

— муаллифнинг фикрича шифр криптобардошлилиги, асосан, калит алмашиш тизимининг бардошлилиги билан белгиланади;

— криптобардошлиликни, раундлар сонини ошириш ҳисобига, исталган поғонага кўтариш мумкин.

Мазкур шифр яратилган муддатидан 2-2,5 йил ўтганлиги боис, унинг криптотаҳлили, калитнинг оптимал қийматлари, модуль арифметикасидан фойдаланиш масалалари ҳақида ҳозирча маълумотлар йўқ.

Кейинги бандда носимметрик шифрлар синфига мансуб машҳур шифрлаш калитларини алмашиш, маълумотларни шифрлаш алгоритмлари ва уларни яратишга асос бўлган муаммолар ҳамда бир томонлама функциялар ҳақида сўз боради.

1.4 Диффи-Хэллман ва RSA бир томонлама функциялари. Махфий калитларни алмашиш ва маълумотларни шифрлаш

У. Диффи ва М. Хэллман ошкора калитлар криптографияси (ошкора криптография) асосчилари экани юқорида айтиб ўтилган эди. Уларнинг бу соҳага оид улкан аҳамиятга молик ихтиролари АҚШ патенти [42-44] ҳисобланади. Унда томонлар ўртасида махфий йўлли бир томонлама функциядан фойдаланиб махфий калитларни бевосита алмашиш муаммоси ҳал

қилиб берилди. Улар бир томонлама функция сифатида махфий кўрсаткичда туб модуль бўйича дискрет даражага ошириш функциясидан фойдаландилар. Модуль арифметикасида бир томонлама функция f нинг махфий аргументи сифатида дискрет даража кўрсаткичи x танланди. Функция қиймати y бўйича катта қийматли туб модуль p арифметикасида x ни топишнинг эффектив ҳисоблаш алгоритми ҳануз топилмаган дискрет логарифм муаммоси билан боғлиқ. [81] да немис олимлари 530 битли туб модуль бўйича дискрет логарифм муаммосини ечганликлари ёритилган. Бу эса дискрет логарифм муаммосига асосланган алгоритмларнинг криптографик бардошлилиги ва хавфсизлик параметрларига бўлган талабларни кучайтиришга олиб келади.

У. Диффи ва М. Хэллман ўзлари номида таърифланган дискрет логарифм муаммосига тенг кучли муаммони ҳам илгари сурдилар:

— агар туб модуль p, $GF(p)$ чекли майдоннинг ҳосил қилувчи (генератор) элементи a ва дискрет даражага ошириш функциялари қийматлари $y_1 \equiv a^{e} (mod\, p)$, $y_2 \equiv a^{d} (mod\, p)$ берилган бўлса, $(a^{e})^{d} (mod\, p) \equiv (a^{d})^{e} (mod\, p)$ топилсин.

Бу ерда $y_1 \equiv a^{e} (mod\, p)$ биринчи томоннинг ошкора калити вазифасини, $y_2 \equiv a^{d} (mod\, p)$ иккинчи томоннинг ошкора калити вазифасини ўтайди. Даража кўрсаткичи e биринчи томоннинг махфий калити вазифасини, даража кўрсаткичи d иккинчи томоннинг махфий калити вазифасини ўтайди. Натурал сон a ва туб модуль p дан таркиб топган жуфтлик (a, p) иккала ёки ундан ортиқ томонлар учун умумий ошкора параметрлардир.

1977 йили яна бир қулай махфий йўлли функцияни танлаб асослаш Массачусетс технология институтининг тадқиқотчилари — Р. Райвест, А. Шамир, Л. Адлеманга насиб этди ва натижада улар томонидан RSA алгоритми [48] ишлаб чиқилди.

RSA криптотизимида модуль n сифатида иккита (ундан ортиқ бўлиши ҳам мумкин) ҳар хил туб сон p, q ларнинг кўпайтмаси бўлган мураккаб модулдан, ошкора шифрлаш калити сифатида n нинг Эйлер пи-функцияси $\varphi(n) = (p-1)*(q-1)$

қиймати бўйича махфий шахсий калит d га ўзаро тескари бўлган даража кўрсаткичи e дан фойдаланилади. Махфий йўл сифатида n нинг туб кўпайтувчи (фактор)лари p, q, ошкора калит сифатида жуфтлик e, n хизмат қилади. Асосий криптографик амал сифатида модуль арифметикасида дискрет даражага ошириш амалидан фойдаланилади.

Носимметрик криптография юзага келган даврнинг бошларида Тоҳир Ал Жамол томонидан таклиф қилинган усулдан [1, 53, 54] шифр яратиш учун ҳам, ЭРИ яратиш учун ҳам фойдаланиш мумкин. Унда Диффи-Хэллман бир томонлама функциясидан фойдаланилган. Тоҳир Ал Жамол шифрида модуль ва асос вазифасида фойдаланиладиган (p, a) — жуфтликдан иборат ошкора калитдан, алоқа каналида i-, j-томонларнинг мос тарзда ўз шахсий калитлари e_i, d_j дан ҳамда алоқа каналида i-, j-томонларнинг мос тарзда ошкора калитлари y_i, y_j дан фойдаланилади; улар умумий маълумотлар базасида сақланиши ёки коммуникация канали орқали томонлараро айирбошланиши мумкин.

Мазкур шифрда ҳар бир шифрлаш сеансида шифрматн муаллифи янги тасодифий сонни генерациялаши лозим бўлади. Шифрматн узунлиги дастлабки матн узунлигига нисбатан икки марта узун бўлиши унинг жиддий камчилигидир.

Полиг-Хэллман криптотизими [1, 7] соф носимметрик эмас. Унда *Диффи-Хэллман бир томонлама функциясидан фойдаланилган.* Модуль сифатида туб ёки таркибли сон бўлган махфий модуль n дан, i-томон билан j - томон учун шифрлаш калити сифатида бир-бирига Эйлер пи-функцияси $\varphi(n)$ бўйича ўзаро тескари бўлган махфий бутун сонлар жуфтлиги (k_{1ij}, k_{2ij}) дан фойдаланилади ва бу ерда кириш ва чиқиш блоклари узунлиги модуль узунлигидан кам бўлмайди.

Ҳозирги замон ошкора криптографиясида эллиптик эгри чизиқ нуқталари бўйича тузилган группаларга эътибор ошган. Бундай группалардан ошкора криптографияда фойдаланишни дастлаб Миллер ва Коблиц таклиф этган. Криптографияда чекли алгебраик структураларда, масалан, чекли майдонларда бе-

рилган эллиптик эгри чизиқлардан фойдаланилади [7, 82]. Туб майдон F_p да берилган эллиптик эгри чизиқ

$$y^2 = x^3 + a*x + b \ (mod\ p) \qquad (1.3)$$

таққосламанинг $P = (x, y)$ нуқталари (ечимлари) тўпламини ташкил этади. Бу ерда a ва b $4*a^3+27*b \neq 0$ $(mod\ p)$ шартини қаноатлантирувчи доимийлар, $p>3$. Тўплам группани ташкил этиши учун унга чексиз узоқлашган $0=(x, \infty)$ нуқта бирлаштирилади, натижада группа ташувчиси $E=\{1.3\ ечимлари\}\ U\{0\}$ кўринишни олади. Мазкур группанинг криптография учун асосий амали нуқталарни такроран m марта қўшиш амали $[m]P$ бўлиб, уни $[m]$ га кўпайтириш деб аталади ва у рекурсив суратда амалга оширилади. Ошкора криптографияда яратилган кўпчилик алгоритмларнинг эллиптиқ эгри чизиқли аналоглари ишлаб чиқилган. Мавжуд алгоритмларнинг асосий устунлиги [82-86] нисбатан кичик калитлардан ва модуллардан фойдаланиб зарур криптобардошлиликни таъминлаб бериш бўлиб, камчилиги кўпайтириш амалини бажариш мураккаблигидадир. Эллиптик эгри чизиқли криптотизимлар криптобардошлилиги эллиптик эгри чизиқларда дискрет логарифмлаш муаммосининг мураккаблиги билан белгиланади. Бу муаммони дискрет логарифм муаммосига келтириш [63] да баён этилган.

Ошкора криптография юзага келгандан буён, бир томонлама криптографик функцияларга қўшимча махфийлик ўрнатишга уринишлар ҳануз давом этмоқда [87]. Лекин, шу кунгача бундай уринишлар ижобий натижага олиб келмаган, туб ва мураккаб модулда ягона махфийликка эга (дискрет логарифм муаммосига нисбатан — даража кўсаткичи, эллиптик чизиқли дискрет логарифм муаммосига нисбатан — кўпайтувчи, факторлаштириш муаммосига нисбатан — туб кўпайтувчи) даражага ошириш функцияси ошкора криптографиянинг асосий бир томонлама функцияси бўлиб қолмоқда. Қўшимча махфийлик ўрнатишга уринишлар хусусида шуни таъкидлаш жоизки, агар бир томонлама даражага ошириш функцияси ёрдамида шифрланган матнга қўшимча ёпиқ параметр, масалан R ни

кўпайтувчи сифатида ўрнатилса, бу параметр шифр очилгандан сўнг осонгина топилади ва ундан фойдаланишдан маъно қолмайди. Бундан буён ҳам ошкора криптографияда бир томонлама криптографик функцияга қўшимча махфийлик ўрнатиш долзарб муаммолардан бири бўлиб қолади.

1.5 Носимметрик криптотизимлар синфига мансуб электрон рақамли имзо схемалари

Криптографлар орасида машҳур электрон рақамли имзони шакллантириш ва уни текшириш алгоритмлари гуруҳига криптобардошлилиги дискрет логарифм ва эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган, АҚШ давлат стандартлари [88], Белорусь Республикасида СТБ 1176.2-99 [89], Украинада ДСТУ 4145-2002 [90], Россия Федерациясида ГОСТ 34.10-94 [1, 2, 91] ва ГОСТ Р 34.10-2001 [92] стандартлари, криптобардошлилиги факторлаштириш муаммосининг мураккаблигига асосланган халқаро стандарт мақомига эга RSA алгоритми киради.

[1] да криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ криптотизимларини умумий схема асосида яратиш мумкинлиги ва ЭРИ учун дастлабки машҳур Тохир Ал Жамол [8] схемаси, К. Шнорр схемаси, АҚШ стандарти DSS [93] бу умумий схеманинг хусусий ҳоллари экани келтирилган. Кейинчалик яратилган кўпгина ЭРИ схемалари [1, 7] ҳам шу умумий схеманинг хусусий ҳоллари бўлиб чиққан.

Тоҳир Ал Жамол схемаси бошқа кўпгина ЭРИ алгоритмларига асос бўлган. К. Шнорр томонидан таклиф этилган p-1 ўрнига унинг катта фактори q дан фойдаланишга асосланган ЭРИ узунлигини камайтириш усули билан бир қаторда, DSS ва ГОСТ 34.10-94 юзага келиши учун асос бўлган [94]. Булар ЭРИ шакллантириш жараёнида k ни тескарилаш амали ишлатилиши сабабли паст эффективликка эгадир. Тоҳир Ал Жамол схемаси ва у каби ЭРИ шакллантиришда дастлабки матн M дан фойдаланадиган алгоритмларнинг яна бир жиддий камчиликлари-

дан бири, бу бузғунчи учун махфий калит x номаълум бўлиб M дан фарқли тасодифий сон бўлган сохта $M_{сохта}$ учун ҳам ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси тўғри бажариладиган сохта ЭРИ ($r_{сохта}$, $s_{сохта}$) шакллантириш мумкинлигидир [8, 14, 94]. Буни олдини олиш мақсадида ҳозирги замонда электрон рақамли имзо алгоритмлари хэш-функциялар [1, 7, 13, 14, 95] ёрдамида амалга оширилади. Дастлабки матн (хабар) M асосида ҳисобланган хэш-функция қиймати $h(M)$ *message digest* — хабар дайджести дейилади. Юқорида келтирилган рақамли имзо шакллантириш ва уни текшириш ифодаларида M ўрнига $m=h(M)$ қўйилади.

ГОСТ Р 34.10-94 алгоритми DSA алгоритмига жуда ўхшаш ва ҳозирда ундан фойдаланиш чекланган. 2001 йилда Россияда электрон рақамли имзонинг янги стандарти қабул қилинган. Унинг криптобардошлилиги етарли даражада юқори бўлиб, эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига ҳамда фойдаланиладиган хэш-функция ГОСТ Р 34.11 [96] нинг бардошлилигига асосланади.

Факторлаштириш муаммосининг мураккаблигига асосланган ЭРИ схемалари қаторига RSA ва ESIGN [1] схемалари киради. RSA криптотизимининг 1.4 да кўрсатилган параметрлари ЭРИ учун ҳам айнан кўринишда фойдаланилади.

RSA рақамли имзоси камчиликлардан ҳам ҳоли эмас. n модулни танлашда RSA рақамли имзоси тизими учун e ва d калитларни катта миқдордаги қўшимча шартлар бўйича албатта текширилиши зарурлиги ва шартлар йилдан-йилга тўлдирилиб борилаётганлиги [97] RSA тизимининг жиддий камчилигидир.

1-бўлим бўйича хулосалар

1. Симметрик шифрлар Клод Шеннонниng фундаментал тамойиллари асосида уларнинг зарур криптобардошлилигини таъминлаш учун хизмат қилувчи амаллардан фойдаланишга асосланган. AESдан бошқа кўпчилик шифрлар мувозанатланган тармоқ архитектурасига эга. Шифрларда фойдаланилган амаллар тўплами модуль арифметикасида бажарилган бўлиб,

XOR, даврий суриш ва ўрнига қўйиш амалларидан фойдаланиш уларнинг барчасига хос. Келтирилган алгоритмлар бир-биридан модуль қиймати ва тури билан фарқланади. Фақат AESда полиномли модуль бўйича матрицавий кўпайтириш амалидан фойдаланилса, қолган алгоритмларда туб ва/ёки мураккаб модуль бўйича қўшиш ва кўпайтириш амалларидан фойдаланилади.

2. ГОСТ-28147-89 дан бошқа симметрик блокли шифрлар синфига мансуб маълумотларни шифрлаш алгоритмларида маълумотларни шифрлашда электрон код китоби, шифрматн орқали тескари боғланиш, шифр блокларнинг илашиши, чиқиш орқали тескари боғланиш ва санокчи каби 5 хил иш маромидан фойдаланиш мумкин. ГОСТ-28147-89да электрон код китоби маромига ўхшаш оддий алмаштириш маромидан, DES, AESга хос маромлардан фарқли бўлган гаммалаштириш, тескари боғланишли гаммалаштириш маромлари ва улардан принципиал фарқли имитоқистирма ишлаб бериш маромидан фойдаланилади. Имитоқистирма ишлаб бериш мароми гаммалаш шифри имитабардошлиликка эга эмаслиги сабабли зарурдир. Гаммалаш реккурент сонлар кетма-кетлиги генератори (РГПЧ) дан фойдаланиши уларни мос ишлашини таъминлаш учун қўшимча маълумотлар узатишни талаб этади.

3. Симметрик шифрларда турли маромлардан амалиётда фойдаланиш қулайликлари ҳар хил. Калитларни ва кириш блоки узунлигига каррали узунликка эга дастлабки матнларни маълумотлар базасида сақлаш учун шифрлашда электрон код китоби иш маромини, алоҳида белгилар учун шифрматн орқали тескари боғланиш иш маромини, алоқа тизими учун эса чиқиш орқали тескари боғланиш иш маромини қўллаш қулай ҳисобланади.

4. Носимметрик криптотизимлар модуль арифметикасида бир томонлама дискрет даражага ошириш функциялари асосида қурилган, уларнинг криптобардошлилиги, асосан, дискрет логарифм, эллиптик эгри чизиқли дискрет логарифм ва факторлаш муаммоларини ҳал этиш мураккаблиги билан белгиланади. Улар асосида шифрлар яратишдан ташқари, асрлар

давомида муаммо бўлиб келган, ҳимояланмаган алоқа канали орқали махфий калитларни алмашиш, аутентификация ва электрон рақамли имзо тизимларини яратиш каби қатор янги имкониятлар пайдо бўлди, ошкора криптография яратилди. Алгоритмларда катта туб сонлардан фойдаланилганлиги уларни ишлаш тезлигини камайтиради ва шифрлашда кенг қўллаш имконини бермайди. Бундай алгоритмлар асосан калит алмашиш тизими мавжуд бўлмаган ва қичик ҳажмдаги маълумотларни шифрлашда қўлланилади.

5. Криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланган мавжуд электрон рақамли имзони шакллантириш ва унинг ҳақиқийлигини тасдиқлаш алгоритмлари умумий схеманинг хусусий ҳоллари бўлиб, уларнинг сони 13000 дан ортиқ. Улар орасида электрон рақамли имзони шакллантириш ва ҳақиқийлигини тасдиқлаш жараёнларида тескарилаш амалидан фойдаланилганлари ҳам мавжуд бўлиб, бу алгоритмларнинг тезлигини пасайишига олиб келади.

6. Ошкора криптография юзага келгандан буён бир томонлама криптографик функцияларга қўшимча махфийлик ўрнатишга кўп уринишлар бўлган. Хорижда яратилган криптотизимларда туб ва мураккаб модулда ягона махфийликка (махфий йўлга) эга бўлган даражага ошириш функцияси ошкора криптографиянинг асосий бир томонлама функцияси сифатида фойдаланилади.

7. Мавжуд электрон рақамли имзони шакллантириш ва ҳақиқийлигини тасдиқлаш алгоритмларида юқори криптобардошлиликка эга хэш-функциялардан фойдаланиш одат тусига кирган, акс ҳолда дастлабки матнга сохта имзо қўйиш имконияти бор.

8. Криптографик миллий стандартлар яратиш бўйича хорижий давлатлар, масалан Россия Федерацияси тажрибаси шуни кўрсатадики, улар миллий стандарт лойиҳасини яратишда прототип танлашда АҚШ стандартларини асос сифатида олиб, унинг камчиликларини бартараф этувчи амаллар комбинациясидан фойдаланган ҳолда, ўз стандартларини яратадилар. Ўзбекистон Республикаси криптографик давлат стандартлари-

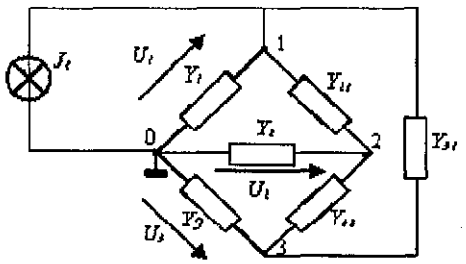
ни яратишда шифр учун прототип сифатида шифрларга қўйиладиган барча талабларга жавоб берувчи AESни, электрон рақамли имзо учун прототип сифатида криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланган умумий схема вариантларидан ҳар сеансда тескарилаш амалидан фойдаланилмайдиганини ёки криптобардошлилиги эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган ГОСТ Р 34.10 — 2001ни асос қилиб олиш мақсадга мувофиқ.

2-БЎЛИМ

ДИАМАТРИЦАЛАР АЛГЕБРАЛАРИ ВА ПАРАМЕТРЛИ АЛГЕБРАИК СТРУКТУРАЛАР

2.1 Такомиллашган диаматрицалар алгебраси

Диаматрицалар алгебраси 1974 йилда т.ф.д., проф. П.Ф. Хасанов томонидан чизиқли электромагнит ва электр занжирлари ҳамда тизимлари анализи ва синтези масалаларини эффектив ечиш учун ишлаб чиқилган эди [10-13]. Бунинг сабаби, матрицалар алгебрасида тузиладиган чизиқли занжирнинг модели диаматрицалар алгебрасида бевосита акс этишидадир. Масалан, 2.1-расмда келтирилган тўрт қутбли электр занжирининг модели матрицалар алгебрасида (2.1) кўринишга эга бўлса, диаматрицалар алгебрасида (2.2) кўринишга эга бўлади.



2.1-расм. Тўрт қутбли электр занжирининг схемаси.

$$\begin{vmatrix} Y_1+Y_{21}+Y_{31} & -Y_{21} & -Y_{31} \\ -Y_{21} & Y_{21}+Y_2+Y_{32} & -Y_{32} \\ -Y_{31} & -Y_{32} & Y_{31}+Y_{32}+Y_{31} \end{vmatrix}_{Y} \times \begin{vmatrix} U_1 \\ U_2 \\ U_3 \end{vmatrix}_{U} = \begin{vmatrix} J_1 \\ 0 \\ 0 \end{vmatrix}_{J} \quad (2.1) \qquad \begin{vmatrix} Y_1 & Y_{21} & Y_{31} \\ Y_{21} & Y_2 & Y_{32} \\ Y_{31} & Y_{32} & Y_3 \end{vmatrix}_{d_2Y} \lozenge_2 \begin{vmatrix} U_1 \\ U_2 \\ U_3 \end{vmatrix}_{U} = \begin{vmatrix} J_1 \\ 0 \\ 0 \end{vmatrix}_{J} \quad (2.1)$$

Бу ерда, $\times$, $\lozenge_2$ - ўзаро мос тарзда, матрицани матрицага, диаматрицани матрицага кўпайтириш амалининг рамзлари. Бунда компонент (элемент)лар диаматрицасидан, яъни d_2-матрицадан, компонентлар матрицасига ўтиш қуйида келтирилган d_2-алмаштириш ёрдамида амалга оширилади:

Матрицанинг ҳар бир бош диагонал элементи d_2-матрица (d_1-матрица)да диагонал элемент жойлашган устун (сатр) элементларининг йигиндисига тенг, матрицанинг ҳар бир нодиа-

гонал элементи d_2-матрица (d_1-матрица)нинг унга жойи бўйича мос элементининг қарама-қарши қийматига тенг.

Бу ҳол матрица детерминантининг символли ифодасини ортиқча қўшилувчи қарама-қарши қийматли жуфтлар (дубликациялар)сиз тузишга имкон берувчи ихчам ёйиш ифодаларига олиб келади [13] ва матрицани тескарилаш алгоритмларини соддалаштиради. Матрицаларни тескарилаш амалларини соддалаштириш маълумотларни шифрлаш алгоритмларини яратишда кўл келади [28].

Диаматрицалар алгебрасида d_l-матрица диадетерминанти (диааниқловчиси) унга d_l-алмаштириш бўйича мос матрица детерминантига сон қиймати бўйича тенг деган қоида асосида ҳисобланади. Бу ерда $l \in \{1,2\}$.

Шуни алоҳида таъкидлаш жоизки, диаматрицалар алгебраси матрицалар алгебрасини ривожлантиришга ҳам ўз ҳиссасини қўшади. Бунга мисол тариқасида, матрица детерминантининг нолга тенг бўлиши ҳақида шу кунгача матрицалар назариясига оид адабиётда эълон қилинмаган қуйидаги хоссани келтириш мумкин:

Хосса: агар mxm тартибли матрицанинг ҳар бир диагонал катакда жойлашган элементи шу катакда жойлашган устун ёки сатр нодиагонал элементлари йигиндисининг қарама-қарши қийматига тенг бўлса, унда бу матрицанинг детерминанти нолга тенг.

Бу хосса шу матрицага мос d_l-матрица учун диадетерминантни диагонал элементлари бўйича ёйиш теоремаси асосида осонгина исботланади. Чунки, бундай d_l-матрицанинг ҳар бир диагонал элементи нолга тенгдир.

Матрица A ни матрица B га, диаматрица d_lA ни матрица B га кўпайтириш амали қуйидаги қоидага бўйсунади:

$$A \times B = d_l A \Diamond_l B, \qquad (2.3)$$

бу ерда $l \in \{1,2\}$.

Натижавий матрица $C=d_lA\Diamond_lB$ га тенг бўлиб, мазкур қоида чизиқли занжирлар модели бўлган чизиқли тенгламалар тизимини акс эттиришни назарда тутган. Лекин, криптография масалалари учун диаматрицалар устида амаллар модуль арифме-

тикасида бажарилиши ва натижа диаматрица шаклида бўлиши қулайдир. Бунинг учун натижавий матрица C устида d_l-алмаштиришнинг бажарилиши етарлидир: $C \Rightarrow d_l C$ [18].

Қуйидаги 2.1 ва 2.2-мисолларда модуль $n=23$ бўлганда, 3-тартибли d_l-матрицани ўзига мос матрицасига кўпайтириб, натижавий d_l-матрица ҳосил қилиш тартиби келтирилган:

2.1-мисол

$$\begin{vmatrix} d_1A \\ 8 & 19 & 6 \\ 13 & 22 & 9 \\ 17 & 0 & 2 \end{vmatrix} \Diamond_1 \begin{vmatrix} A \\ 10 & 4 & 17 \\ 10 & 21 & 14 \\ 6 & 0 & 19 \end{vmatrix} \equiv \begin{vmatrix} C \\ 12 & 9 & 20 \\ 3 & 21 & 17 \\ 13 & 1 & 3 \end{vmatrix} \Rightarrow \begin{vmatrix} d_1C \\ 18 & 14 & 3 \\ 20 & 18 & 6 \\ 10 & 22 & 17 \end{vmatrix}$$

2.2-мисол

$$\begin{vmatrix} d_2A \\ 3 & 19 & 6 \\ 13 & 2 & 9 \\ 17 & 0 & 4 \end{vmatrix} \Diamond_2 \begin{vmatrix} A \\ 10 & 4 & 17 \\ 10 & 21 & 14 \\ 6 & 0 & 19 \end{vmatrix} \equiv \begin{vmatrix} C \\ 12 & 9 & 20 \\ 3 & 21 & 17 \\ 13 & 1 & 3 \end{vmatrix} \Rightarrow \begin{vmatrix} d_2C \\ 5 & 14 & 3 \\ 20 & 18 & 6 \\ 10 & 22 & 17 \end{vmatrix}$$

Демак, натижавий d_l-матрицани шакллантириш учун модуль арифметикасида $\Diamond_1$ ва d_l амаллари кетма-кетлигини бажариш лозим. Бу амални A ни унга мос бўлган d_lA билан алмаштиришни ҳам ҳисобга олган ҳолда, $®_l$ рамзи билан белгилаб, уни d_l-матрицаларни кўпайтириш амали деб номлаймиз.

Кўпайтириш амали икки хил бўлиши мумкин:

$$®_l \in \{®_1, ®_2\}.$$

mxm тартибли d_l- матрицалар d_lA, d_lB, d_lC m сатр ва m устундан тузилган бўлгани учун c-сатр ва u-устунда жойлашган элементларни мос тарзда $a[c,u]$, $b[c,u]$, $c[c,u]$ ёки a_{cu}, b_{cu}, c_{cu} билан белгилаймиз, бу ерда $0 \le c, u < m$. (2.4) да модуль n бўйича mxm-тартибли d_l— матрицаларнинг кўпайтириш ифодалари келтирилган.

$$\begin{vmatrix} a[0,0] & \dots & a[0,u] & \dots & a[0,m-1] \\ a[1,0] & \dots & a[1,u] & \dots & a[1,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ a[c,0] & \dots & a[c,u] & \dots & a[c,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ a[m-1,0] & \dots & a[m-1,u] & \dots & a[m-1,m-1] \end{vmatrix} ®_l \begin{vmatrix} b[0,0] & \dots & b[0,u] & \dots & b[0,m-1] \\ b[1,0] & \dots & b[1,u] & \dots & b[1,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ b[c,0] & \dots & b[c,u] & \dots & b[c,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ b[m-1,0] & \dots & b[m-1,u] & \dots & b[m-1,m-1] \end{vmatrix} \equiv$$

$$\equiv \begin{vmatrix} c[0,0] & \dots & c[0,u] & \dots & c[0,m-1] \\ c[1,0] & \dots & c[1,u] & \dots & c[1,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ c[c,0] & \dots & c[c,u] & \dots & c[c,m-1] \\ \dots & \dots & \dots & \dots & \dots \\ c[m-1,0] & \dots & c[m-1,u] & \dots & c[m-1,m-1] \end{vmatrix} \quad (2.4)$$

Натижавий диаматрица $d_lC_l \equiv d_lA \circledR d_lB$ $(mod\ n)$ элементлари $l=1$, $l=2$ ҳоллар учун ва диагонал ҳамда нодиагонал элементлар учун турлича ифодалар асосида ҳисобланади.

$l=1$ ҳол учун қуйидаги (2.5) ва (2.6) таққосламалар ўринлидир [18]:

$$c[c,c] \equiv b[c,c]*\Sigma^{m-1}_{j=0} a[c,j] - \Sigma^{m-1}_{j=0,\ j\neq c} a[c,j]*b[j,j]\ (mod\ n), \quad (2.5)$$

$$c[c,u]_{c\neq u} \equiv a[c,u]*\Sigma^{m-1}_{j=0} b[u,j] + b[c,u]* *\Sigma^{m-1}_{j=0} a[c,j] - \Sigma^{m-1}_{i=0;\ i\neq c,u} a[c,i]*b[i,u]\ (mod\ n). \quad (2.6)$$

$l=2$ ҳол учун қуйидаги (2.7) ва (2.8) таққосламалар ўринлидир:

$$c[u,u] \equiv a[u,u]*\Sigma^{m-1}_{i=0} b[i,u] - \Sigma^{m-1}_{i=0,\ i\neq c} a[i,i]*b[i,u]\ (mod\ n) \quad (2.7)$$

$$c[c,u]_{c\neq u} \equiv a[c,u]*\Sigma^{m-1}_{i=0} b[i,u] + b[c,u]*\Sigma^{m-1}_{i=0} a[i,u] - \Sigma^{m-1}_{i=0;\ i\neq c,u} a[c,i]*b[i,u]\ (mod\ n). \quad (2.8)$$

Келтирилган (2.5-2.8) ифодалар бўйича ҳисоблашларни бажаришда аввало

$l=1$ ҳол учун $a_d[c,j] \equiv \Sigma^{m-1}_{j=0} a[c,j]$ $(mod\ n)$, $b_d[c,j] \equiv \Sigma^{m-1}_{j=0} b[c,j]$ $(mod\ n)$,

$l=2$ ҳол учун $b_d[i,u] \equiv \Sigma^{m-1}_{j=0} b[i,u]$ $(mod\ n)$, $a_d[i,u] \equiv \Sigma^{m-1}_{j=0} a[i,u]$ $(mod\ n)$ ларни берилган диаматрицаларга тегишли диаматрицаларнинг диагонал элементлари сифатида ҳисоблаб, сўнгра улардан бир неча бор фойдаланиш ҳисоблашлар эффективлигини оширади.

Қуйидаги 2.3- ва 2.4-мисолларда, модуль $n=23$ бўлганда, 3-тартибли d_l-матрицаларнинг кўпайтмаси коммутативлик хоссасига эга эмаслиги акс этган:

2.3-мисол

$$\begin{vmatrix} d_1A & & \\ 3 & 12 & 17 \\ 16 & 4 & 18 \\ 7 & 13 & 5 \end{vmatrix} \circledR_1 \begin{vmatrix} d_1B & & \\ 2 & 6 & 17 \\ 17 & 13 & 7 \\ 5 & 7 & 8 \end{vmatrix} \equiv \begin{vmatrix} d_1C & & \\ 2 & 11 & 18 \\ 13 & 19 & 9 \\ 10 & 16 & 17 \end{vmatrix}, \quad \begin{vmatrix} d_1B & & \\ 2 & 6 & 17 \\ 17 & 13 & 7 \\ 5 & 7 & 8 \end{vmatrix} \circledR_1 \begin{vmatrix} d_1A & & \\ 3 & 12 & 17 \\ 16 & 4 & 18 \\ 7 & 13 & 5 \end{vmatrix} \equiv \begin{vmatrix} d_1C & & \\ 12 & 8 & 6 \\ 6 & 16 & 0 \\ 4 & 6 & 11 \end{vmatrix}$$

2.4-мисол

$$\begin{vmatrix} d_2A & & \\ 3 & 12 & 17 \\ 16 & 4 & 18 \\ 7 & 13 & 5 \end{vmatrix} \circledR_2 \begin{vmatrix} d_2B & & \\ 2 & 6 & 17 \\ 17 & 13 & 7 \\ 5 & 7 & 8 \end{vmatrix} \equiv \begin{vmatrix} d_2C & & \\ 2 & 4 & 5 \\ 5 & 5 & 1 \\ 9 & 1 & 12 \end{vmatrix}, \quad \begin{vmatrix} d_2B & & \\ 2 & 6 & 17 \\ 17 & 13 & 7 \\ 5 & 7 & 8 \end{vmatrix} \circledR_2 \begin{vmatrix} d_2A & & \\ 3 & 12 & 17 \\ 16 & 4 & 18 \\ 7 & 13 & 5 \end{vmatrix} \equiv \begin{vmatrix} d_2C & & \\ 18 & 11 & 14 \\ 4 & 19 & 22 \\ 12 & 7 & 6 \end{vmatrix}$$

Диаматрицалар алгебраси учун алгебра ташувчиси квадрат матрицаларнинг чекли тўпламига эга бўлиб, алгебра амаллари тўплами диаматрицаларни тескарилаш "-1", транспонирлаш "t" амалларини ҳамда бирлик E ва ноль 0 элементларини ўз таркибига олади.

Шуни таъкидлаб ўтиш керакки, диаматрицани тескарилаш "-1" амали фақатгина унинг детерминанти 0 дан фарқли бўлгандагина амалга оширилиши мумкин. Диаматрицани тескарилаш натижасида унга d_i -алмаштириш бўйича мос бўлган матрицага тескари матрица ҳосил бўлади. Яъни, агар $d_iA = A$, $det\, A \neq 0$ бўлса, унда $(d_iA)^{-1} = A^{-1}$.

Шунинг учун тескари матрицадан диаматрицага ўтиш учун қуйидаги (2.9) ва (2.10) ифодаларга асосан, d_i-алмаштиришни бажариш лозим бўлади:

$$(d_1A)^{\backslash\backslash -1} = d_1((d_1A)^{-1}), \qquad (2.9)$$

$$(d_2A)^{\backslash -1} = d_2((d_2A)^{-1}). \qquad (2.10)$$

Диаматрицани тескарилаш "-1" ва d_1-алмаштиришдан иборат амаллар кетма-кетлиги "$\backslash -1$" билан, "-1" ва d_2-алмаштиришдан иборат амаллар кетма-кетлиги "$\backslash\backslash -1$" билан белгиланади.

Шунингдек, матрицани транспонирлаш ^{t} амали d_i-матрица устида бажарилганда транспонирланган d_i-матрицани ҳосил этиш учун $(d_i,\ ^t,\ d_i)$ учликдан иборат кетма-кет алмаштиришларни бажариш лозим. $d_i,\ ^t,\ d_i$-алмаштиришлардан иборат амаллар кетма-кетлигини "tt" билан белгилаб, $d_2,\ ^t,\ d_2$-

алмаштиришлардан иборат амаллар кетма-кетлигини " $t2$ " билан белгилаймиз.

Диаматрицани транспонирлаш амаллари $l=1$, $l=2$ ҳоллар учун натижавий диаматрица C матрицани транспонирлаш амалидан қўшимча суратда фақат диагонал элементларни ҳисоблаш ифодалари билан фарқ қилади.

$l=1$ ҳол учун қуйидаги (2.11) таққослама ўринлидир:

$$c[c,c] \equiv \Sigma^{m-1}_{j=0} a[c,j] + \Sigma^{m-1}_{i=0,\, i\neq c} (n-a[i,\, c])\ (mod\ n). \quad (2.11)$$

$l=2$ ҳол учун қуйидаги (2.12) таққослама ўринлидир:

$$c[c,c] \equiv \Sigma^{m-1}_{i=0} a[i,\, c] + \Sigma^{m-1}_{j=0,\, j\neq c} (n-a[c,j])\ (mod\ n). \quad (2.12)$$

Диаматрицани транспонирлаш амалларини бажаришда диагонал элементлар учун қуйидаги хоссалар ўринлидир:

$diagonal(d_1A) \equiv diagonal\ ((d_2A)^{t2})$,

$diagonal(d_2A) \equiv diagonal\ ((d_1A)^{t1})$.

Қуйидаги 2.5- ва 2.6-мисолларда модуль $n=23$ бўлганда, 3-тартибли d_l-матрицаларнинг транспонирлаш натижалари акс этган:

2.5-мисол

$$d_1A = \begin{vmatrix} 9 & 2 & 3 \\ 14 & 17 & 7 \\ 5 & 19 & 13 \end{vmatrix} \Rightarrow (d^1A)^{t1} = \begin{vmatrix} 18 & 14 & 5 \\ 2 & 17 & 19 \\ 3 & 7 & 4 \end{vmatrix}$$

2.6-мисол

$$d_2A = \begin{vmatrix} 18 & 2 & 3 \\ 14 & 17 & 7 \\ 5 & 19 & 4 \end{vmatrix} \Rightarrow (d_2A)^{t2} = \begin{vmatrix} 9 & 14 & 5 \\ 2 & 17 & 19 \\ 3 & 7 & 13 \end{vmatrix}$$

Диаматрицалар алгебрасини криптография масалалари учун татбиқ этиш учун уни юқорида баён этилган ҳолда такомиллаштириб, такомиллашган диаматрицалар алгебрасига қуйидагича таъриф бериш мақсадга мувофиқ [18]:

Таъриф. $\check{D}$ — чекли, яъни, n та элементдан иборат бутун сонлар майдони устида аниқланган квадрат диаматрицалар чекли тўплами, $\Omega = \{+, \circledR_l, d_l, {}^{t1}, {}^{t2}, {}^{\backslash\backslash -1}, {}^{\backslash -1}, E, 0\}$ — $\check{D}$ устида аниқланган алгебраик амаллар тўплами бўлса, $(\check{D};\ \Omega)$ — жуфтлик диаматрицалар алгебраси деб аталади; бу ерда ўзаро мос тарзда + — қўшиш, $\circledR_l$ — кўпайтириш, $\circledR_l \in \{\circledR_1,\ \circledR_2\}$, d_l — алмаштириш, ${}^{t1}, {}^{t2}$ — транспонирлаш, ${}^{\backslash\backslash -1}, {}^{\backslash -1}$ — тескарилаш амалларининг, E — бирлик элементининг, 0 — ноль элементининг рамзларидир.

Мазкур такомиллашган диаматрицалар алгебраси [10-13] да келтирилган алгебрадан амаллар чекли тўплам устида берилган диаматрицалар тўплами устида аниқланиши, барча амаллар диаматрицалар тўплами устида аниқланиб диаматрица ҳосил этилиши билан фарқланади.

Мазкур алгебра криптология масалаларини ечиш учун қулайлигига кейинги бўлимларда ишонч ҳосил қилиш мумкин.

Диаматрицавий кўпайтириш амали матрицавий кўпайтириш амалига нисбатан мукаммал шифрлар яратиш муаммоси нуқтаи назаридан қулай эканлигини илмий криптология асосчиси Клод Шеннонниng [37], мукаммал шифр яратишда ишлатиладиган алмаштиришлар яхши аралашиш ва кенг ёйилишга олиб келиши лозимлиги ҳақидаги тавсиялари кўпроқ мос келишини қуйидаги мисолдан кўриш мумкин.

2.7-, 2.8- ва 2.9-мисолларда модуль $n=256$ бўлганда 4-тартибли d_1-матрицаларнинг ва матрицаларнинг 1 тадан элементлари ўзгарганда натижавий матрицаларда ўзгарган соҳалар акс этган:

2.7-мисол: d_1-матрицавий кўпайтма

$$\begin{vmatrix} d_1A & & & \\ 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_1 \begin{vmatrix} d_1B & & & \\ 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} d_1C & & & \\ 63 & 228 & 72 & 210 \\ 255 & 31 & 128 & 48 \\ 175 & 119 & 191 & 123 \\ 131 & 84 & 66 & 217 \end{vmatrix}$$

$$\begin{vmatrix} d_1A' & & & \\ 1 & 2 & 3 & 4 \\ 12 & 10 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_1 \begin{vmatrix} d_1B & & & \\ 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} d_1C'' & & & \\ 63 & 228 & 72 & 210 \\ 3 & 36 & 135 & 56 \\ 175 & 119 & 191 & 123 \\ 131 & 84 & 66 & 217 \end{vmatrix}$$

$$\begin{vmatrix} d_1A & & & \\ 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_1 \begin{vmatrix} d_1B' & & & \\ 17 & 1 & 2 & 3 \\ 4 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} d_1C'' & & & \\ 61 & 230 & 72 & 210 \\ 255 & 73 & 128 & 48 \\ 175 & 136 & 174 & 123 \\ 131 & 102 & 66 & 199 \end{vmatrix}$$

2.8-мисол: d_2-матрицавий кўпайтма

d_2A					d_2B					d_2C			
1	2	3	4		17	1	2	3		92	14	111	224
12	9	21	0	®$_2$	4	5	7	8	≡	255	83	9	80
13	17	6	31		9	10	11	12		107	141	10	206
14	18	29	9		13	14	15	16		73	84	241	204

d_2A'					d_2B					d_2C'			
1	2	3	4		17	1	2	3		88	14	111	224
12	10	21	0	®$_2$	4	5	7	8	≡	3	113	16	88
13	17	6	31		9	10	11	12		107	141	3	206
14	18	29	9		13	14	15	16		73	84	241	196

d_2A					d_2B'					d_2C'''			
1	2	3	4		17	1	2	3		92	16	111	224
12	9	21	0	®$_2$	4	6	7	8	≡	255	92	9	80
13	17	6	31		9	10	11	12		107	158	10	206
14	18	29	9		13	14	15	16		73	102	241	204

2.9-мисол: Матрицавий кўпайтма

A					B					C			
1	2	3	4		17	1	2	3		104	97	109	119
12	9	21	0	x	4	5	7	8	≡	173	11	62	104
13	17	6	31		9	10	11	12		234	80	164	231
14	18	29	9		13	14	15	16		176	8	96	166

A'					B					C'			
1	2	3	4		17	1	2	3		104	97	109	119
12	10	21	0	x	4	5	7	8	≡	177	16	69	112
13	17	6	31		9	10	11	12		234	80	164	231
14	18	29	9		13	14	15	16		176	8	96	166

Мисоллардан кўриниб турибдики, диаматрицавий кўпайтма натижасида d_1A нинг *1* та элементи ўзгарганда d_1C да *1* та сатр элементлари, яъни *4* та, d_1B нинг *1* та элементи ўзгарганда эса *7* та элемент ўзгарган; d_2A нинг *1* та элементи ўзгарганда d_2C да *7* та, d_2B нинг *1* та элементи ўзгарганда эса *1* та устун элементлари ўзгарган; матрицавий кўпайтмада эса *1* та устун ёки сатр элементлари, яъни *4* та элемент ўзгарган.

d_1 (d_2)-матрицавий кўпайтмада қатнашувчи ўнг (чап) диаматрицада *1* та элемент ўзгарса, натижавий диаматрицада

ўзгарадиган элементлар сони диаматрица тартибига, тузилмасига, ўзгарган элемент адресига боғлиқ бўлиб, *4x4* тартибли диаматрицалар учун нодиагонал элемент ўзгарса *6* та (матрицавий кўпайтмага нисбатан *1,5* баравар кўп), диагонал элемент ўзгарса *7* та (матрицавий кўпайтмага нисбатан *1,75* баравар кўп) бўлади. Чап (ўнг) диаматрицада *1* та элемент ўзгарса кўпайтмада ўзгарадиган элементлар сони матрицавий кўпайтмадаги каби, одатда, *4* та бўлади.

Қуйидаги 2.10-мисолда модуль *n=256* бўлганда *4*-тартибли d_2-матрицанинг *1* та элементи *1* битга ўзгарганда шифрлашнинг иккинчи босқичида натижавий d_2-матрицада ўзгарган соҳалар акс этган:

2.10-мисол: Икки боскичли d_2-матрицавий кўпайтма

d_2A					d_2B					d_2C			
1	2	3	4		17	1	2	3		92	14	111	224
12	9	21	0	$®_2$	4	5	7	8	≡	255	83	9	80
13	17	6	31		9	10	11	12		107	141	10	206
14	18	29	9		13	14	15	16		73	84	241	204

d_2B					d_2C					d_2C'			
17	1	2	3		92	14	111	224		219	134	175	18
4	5	7	8	$®_2$	255	83	9	80	≡	233	13	239	142
9	10	11	12		107	141	10	206		198	109	85	162
13	14	15	16		73	84	241	204		171	111	83	86

2.11-мисол: Икки босқичли d_2-матрицавий кўпайтма (*1* элемент *1* битга ўзгарган)

d_2A					d_2B					d_2C''			
1	2	3	4		17	1	2	3		92	15	113	227
12	9	21	0	$®_2$	4	5	7	8	≡	255	83	9	80
14	17	6	31		9	10	11	12		150	140	10	203
14	18	29	9		13	14	15	16		73	84	241	204

d_2B					d_2C''					d_2C'''			
17	1	2	3		92	15	113	227		221	179	9	153
4	5	7	8	$®_2$	255	83	9	80	≡	104	7	245	151
9	10	11	12		150	140	10	203		42	65	73	30
13	14	15	16		73	84	241	204		85	113	87	68

2.11-мисолдан кўриниб турибдики, диаматрицавий кўпайтма натижасида d_2A нинг *1* та элементи *1* битга ўзгарганда, шифрлашнинг иккинчи босқичидаёқ барча элементлар ўзгарган.

1-иловада модуль $n=256$ учун *4*-тартибли d_2-матрицаларнинг *1*, *2* тадан элементлари ўзгарганда, натижавий матрицаларда ўзгариш соҳалари ва d_2 - матрицанинг *1* та элементи ўзгарганда шифрлашнинг иккинчи босқичида натижавий d_2-матрицада ўзгарган соҳалар акс этган.

Диаматрицалар асосида шифр яратишда кўпайтмада қатнашувчи диаматрицалардан қай бири доимий бўлса у d_1-матрицавий кўпайтмада чап, d_2-матрицавий кўпайтмада эса ўнг диаматрица сифатида қатнашиши матрицавий кўпайтмага нисбатан оз сонли раундларда лавина эффекти [76] содир бўлиш имконини беради.

Такомиллашган диаматрицалар алгебрасида диаматрицаларни тескарилаш амалини соддалаштиришга имкон берувчи диаматрицани танлаш жуда мухимдир. Бу талабга махсус ва содда тузилмали диаматрицалар жавоб беради.

2.2 Махсус тузилмали диаматрицалар

Махсус тузилмали d_1-матрицалар учун унга мос матрицанинг детерминантини ҳар қандай катта тартибга эга бўлган диаматрица учун осон ҳисоблаш формуласи [17] да келтирилган. Махсус тузилмали диаматрицалардан мураккаб электрон схемалар синтезида фойдаланишга бағишланган тадқиқот натижалари [98] да келтирилган.

Таъриф. Агар берилган mxm тартибли d_2-матрица (d_1-матрица)нинг барча диагонал элементлари бир-бирига тенг ва биринчи сатр (устун)дан бошлаб, то $m-2$ сатр (устун)ларда, ҳар бир сатр (устун) бошидаги элемент шу сатр (устун) диагонал элементидан ўнгда шу сатр (устун)да жойлашган барча элементларга тенг бўлса, ундай d_1 - матрица махсус тузилмали d_2 -матрица (d_1 -матрица) деб аталади [10].

Бундан буён диаалмаштириш деганда d_2 -алмаштириш, диаматрица деганда d_2 -матрица назарда тутилади ва A матрицага мос диаматрица dA, диаматрицаларни бир-бирига кўпайтириш

рамзи $®_2$, диаматрицани тескарилаш рамзи $^{-1}$, уни транспонирлаш рамзи ^{t} билан белгиланади.

(2.13) да *mxm* тартибли махсус тузилмали диаматрица келтирилган.

$$\begin{array}{c|cccccc|} c & & & & & & \\ 0 & a_{00} & a_{01} & a_{02} & \dots & a_{0(m-2)} & a_{0(m-1)} \\ 1 & a_{10} & a_{00} & a_{10} & \dots & a_{10} & a_{10} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ m-2 & a_{(m-2)0} & a_{(m-2)1} & a_{(m-2)2} & \dots & a_{00} & a_{(m-2)0} \\ m-1 & a_{(m-1)0} & a_{(m-1)1} & a_{(m-1)2} & \dots & a_{(m-1)(m-2)} & a_{00} \end{array} \qquad (2.13)$$

Махсус тузилмали диаматрицанинг диадетерминанти қуйидаги (2.14) ифода бўйича ҳисобланади:

$$\Delta \equiv a_{00} * \prod^{m-1}_{j=1} (a_{j(j+1)} + \Sigma^{m-1}_{i=0} a_{ij}) (mod\ n). \qquad (2.14)$$

(2.15) да *4x4* тартибли махсус тузилмали диаматрица келтирилган. Унда барча диагонал элементлар бир-бирига тенг бўлиб, *c=1* сатридаги нодиагонал элементлар бир-бирига тенг ва *c=2* сатри бошида ва сатр сўнгида жойлашган элементлар бир-бирига тенгдир. Келтирилган махсус тузилмали диаматрица *10* хил элемент, яъни $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ элементлар асосида шаклланган.

$$\begin{array}{c|cccc|} c & & & & \\ 0 & a_7 & a_0 & a_1 & a_2 \\ 1 & a_8 & a_7 & a_8 & a_8 \\ 2 & a_9 & a_3 & a_7 & a_9 \\ 3 & a_4 & a_5 & a_6 & a_7 \end{array} \qquad (2.15)$$

Махсус тузилмали диаматрицанинг аҳамиятли томони шундаки, диаматрицалар учун унга мос матрицанинг детерминанти диаматрица элементлари бўйича содда формула орқали ҳисобланиб, бу ўз навбатида шифрлаш ва шифрни очишда муҳим бўлган матрицаларни тескарилаш амалларини соддалаштириб беради. Шу билан бир қаторда, махсус тузилмали диаматрицанинг тескариланиш шартларини аниқлаш жараёни соддалашади. Бу эса, берилган ҳар қандай махфий шифрлаш калити асосида, мураккаб модуль бўйича тескариланиши шарт бўлган диаматрицани шакллантириш имконини яратади [28].

mxm тартибли махсус тузилмали диаматрицанинг диадетерминанти унинг диаалмаштириш натижаси бўлган матрицанинг детерминантига тенг бўлиб, у махсус тузилмали диаматрица диагонал элементи билан *m-1* та кўпайтувчининг кўпайтмасига тенг. Кўпайтувчиларнинг ҳар бири *j*-устун диагонал элементига тегишли бўлиб, бу ерда $j \in \{1,2,..\ m-1\}$. *j*-устунга тегишли кўпайтувчи шу устунда жойлашган барча элементлар билан устун диагонал элементи билан сатр бўйича жойлашган ўнг томондан қўшни элементнинг йиғиндисидан таркиб топган.

Юқорида (2.15) келтирилган *4x4* тартибли махсус тузилмали матрицанинг модуль *p* бўйича ҳисобланган диадетерминанти Δ қуйидаги (2.16) ифода бўйича ҳисобланади:

$$\Delta \equiv a_7*(a_7+a_0+a_8+a_3+a_5)*(a_{7+}a_1+a_8+a_9+a_6)* \\ *(a_7+a_2+a_8+a_9+a_4)\ (mod\ p) \qquad (2.16)$$

Махсус тузилмали диаматрицанинг модуль *p* жуфт қийматли бўлганда тескариланиш шартини таъминлаш, диагонал ва *m-1* та кўпайтувчиларнинг ҳар бирини қийматини модуль *2* бўйича *1* га тенглигини таъминлашга келтирилади.

2.3 Содда тузилмали диаматрицалар

Таъриф. Агар берилган *mxm* тартибли махсус тузилмали диаматрицанинг барча диагонал элементлари бирга тенг ва ҳар бир сатрда шу сатр учун махсус тузилмали диаматрицанинг нодиагонал элементлари бир-бирига тенг бўлса, ундай диаматрица содда тузилмали диаматрица деб аталади [17].

Умумий ҳолда, содда тузилмали диаматрицалар кўпайтмаси коммутативлик хоссасига эга эмас. Содда тузилмали диаматрицалар кўпайтмаси коммутативлик хоссасига эга бўлиши учун улар умумий асосга эга бўлиши шарт.

Таъриф. Агар берилган икки тенг ўлчамли содда тузилмали диаматрицанинг нодиагонал элементларидан ҳар бири иккинчисининг скаляр сонга кўпайтмасига тенг бўлса, бундай содда тузилмали диаматрицалар тенг асосли содда тузилмали диаматрицалар деб аталади.

Қуйидаги 2.12 ва 2.13 мисолларда модуль $n=23$ бўлганда 3-тартибли тенг асосли содда тузилмали диаматрицалар dA ва dB кўпайтмаси dC коммутативлик хоссасига эга бўлиши акс этган:

2.12-мисол

$$\begin{vmatrix} 1 & 19 & 19 \\ 12 & 1 & 12 \\ 17 & 17 & 1 \end{vmatrix}_{dA} \circledR_2 \begin{vmatrix} 1 & 7 & 7 \\ 2 & 1 & 2 \\ 22 & 22 & 1 \end{vmatrix}_{dB} \equiv \begin{vmatrix} 1 & 17 & 17 \\ 18 & 1 & 18 \\ 14 & 14 & 1 \end{vmatrix}_{dC}$$

2.13-мисол

$$\begin{vmatrix} 1 & 7 & 7 \\ 2 & 1 & 2 \\ 22 & 22 & 1 \end{vmatrix}_{dB} \circledR_2 \begin{vmatrix} 1 & 19 & 19 \\ 12 & 1 & 12 \\ 17 & 17 & 1 \end{vmatrix}_{dA} \equiv \begin{vmatrix} 1 & 17 & 17 \\ 18 & 1 & 18 \\ 14 & 14 & 1 \end{vmatrix}_{dC}$$

Қуйидаги 2.14-мисолда модуль $n=23$ бўйича 3х3 тартибли диаматрица dA_нинг 1 дан 23 гача даража қийматлари парчаси келтирилган.

2.14-мисол

1	2	3	4	..	8	9	10	11
1 19 19	1 12 12	1 17 17	1 20 20	..	1 11 11	1 21 21	1 4 4	1 3 3
9 1 9	19 1 19	2 1 2	1 1 1	..	4 1 4	16 1 16	14 1 14	22 1 22
13 13 1	7 7 1	8 8 1	4 4 1	..	16 16 1	18 18 1	10 10 1	19 19 1
12	13	14	15	..	20	21	22	23
1 7 7	1 14 14	1 9 9	1 6 6	..	1 5 5	1 22 22	1 0 0	1 19 19
13 1 13	3 1 3	20 1 20	21 1 21	..	6 1 6	8 1 8	0 1 0	9 1 9
6 6 1	12 12 1	11 11 1	15 15 1	..	1 1 1	9 9 1	0 0 1	13 13 1

Содда тузилмали диаматрицада (2.17) диагонал элемент информатив бўлмагани сабабли, у ахборот узатишда ва уни ифода этишда қатнашмайди, бироқ ахборотга ишлов бериш жараёнларида фаол иштирок этади. Шуни ҳисобга олган ҳолда, mхm тартибли содда тузилмали диаматрица dA ни mх1 тартибли диаматрица-устун $\underline{A}$ билан ифодалашга келишиб оламиз. mх1 тартибли диаматрица-устунлар $\underline{A}$, $\underline{B}$, $\underline{C}$ m сатр (қатор) ва 1 устундан тузилган бўлгани учун c-сатр жойлашган элементларини мос тарзда a_c, b_c, c_c билан белгилаймиз; бу ерда $0 \le c < m$.

$$\begin{vmatrix} 1 & a_0 & a_0 & \dots & a_0 & a_0 \\ a_1 & 1 & a_1 & \dots & a_1 & a_1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m-2} & a_{m-2} & a_{m-2} & \dots & 1 & a_{m-2} \\ a_{m-1} & a_{m-1} & a_{m-1} & \dots & a_{m-1} & 1 \end{vmatrix}_{dA} \Leftrightarrow \begin{vmatrix} a_0 \\ a_1 \\ \dots \\ a_{m-2} \\ a_{m-1} \end{vmatrix}_{\underline{A}} \qquad (2.17)$$

Шуни таъкидлаш жоизки, *mxm* тартибли содда тузилмали диаматрица *A*, *B* ларнинг бошланғич сатрдаги a_0, b_0 элементларидан бошқа барча сатрлар жойлашган нодиагонал элементлари *0* га тенг бўлса, унда бундай диаматрицаларни бир-бирига кўпайтириш натижаси $C \equiv A\circledR_2 B\ (mod\ n)$да ҳам бошланғич сатрдаги c_0 элементидан бошқа барча сатрларда жойлашган элементлар *0* га тенг бўлади. Бундай тузилмага эга диаматрицада *0* элемент информатив бўлмагани сабабли, у ахборот узатишда, алмаштиришларда ва уни ифода этишда қатнашмайди. Шуни эътиборга олган ҳолда бундай диаматрицани битта элементдан тузилган, *1x1* тартибли диаматрица-устун, яъни скаляр сон деб қараш ўринли бўлади. *1x1* тартибли диаматрица-устун (2.18) аслида *1x2* тартибли *1* ва a_0 элементларидан тузилган диаматрицанинг моделидир:

$$\begin{vmatrix} dA \\ 1 \end{vmatrix} \begin{vmatrix} \\ a_0 \end{vmatrix} \Leftrightarrow \begin{vmatrix} \underline{A} \\ a_0 \end{vmatrix} \qquad (2.18)$$

2.4 Диаматрица-устунлар алгебраик структураси

Диаматрица-устунлар $\underline{A}, \underline{B}$ нинг модуль *n* бўйича кўпайтмаси бўлган натижавий диаматрица-устун куйидагича (2.19) ифодаланади [16]:

$$\underline{C} \equiv \underline{A}\circledR_3 \underline{B}\ (mod\ n). \qquad (2.19)$$

Иккита $\underline{A}$ ва $\underline{B}$ диаматрица-устун *c*-сатр элементлари a_c ва b_c устида модуль *n* бўйича параметрли кўпайтириш ифодаси қуйидаги (2.20) таққослама кўринишига эга:

$c \in \{0,1,...m\text{-}1\}$ учун

$$c_c \equiv a_c\circledR_3 b_c\ (mod\ n) \equiv a_c + (1+R)^* b_c\ (mod\ n). \qquad (2.20)$$

Бу ерда $\circledR_3$ — устунлараро параметрли кўпайтириш амалининг рамзи.

Бундан буён мазкур амални, анъанавий кўпайтириш ва диаматрицавий кўпайтириш амалларидан фарқли эканини ҳисобга олган ҳолда, устунлараро параметрли кўпайтириш амали деб атаймиз.

Бу ерда R параметр деб аталади ва $R \equiv (a_0 + a_1 + .. a_{m-2} + a_{m-1}) \pmod n$ бўйича ҳисобланади.

Келтирилган ифода қуйидаги (2.21) қоидага мувофиқ аниқланади:

$$\begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \circledR_3 \begin{vmatrix} b_0 \\ b_1 \\ . \\ b_{m-2} \\ b_{m-1} \end{vmatrix} \equiv \begin{vmatrix} c_0 \\ c_1 \\ . \\ c_{m-2} \\ c_{m-1} \end{vmatrix} \equiv \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} + (1+R) * \begin{vmatrix} b_0 \\ b_1 \\ . \\ b_{m-2} \\ b_{m-1} \end{vmatrix} \qquad (2.21)$$

Диаматрица-устунлар устида параметрли кўпайтириш амали матрица-устунлар устида кўпайтириш амалига нисбатан мукаммал шифрлар яратиш муаммоси нуқтаи назаридан кулай эканлигини мукаммал шифр яратишда ишлатиладиган алмаштиришлар яхши аралашиш ва кенг ёйилишга олиб келиши лозимлиги ҳақидаги тавсиялари кўпроқ мос келади. Кириш диаматрица-устунини доимий диаматрица-устунга параметрли кўпайтиришга асосланган шифралмаштиришларда киришда *1* та элемент ўзгариши чиқишда матрица-устунни скалярга кўпайтмаси чиқишидагига нисбатан $(m-1)$ марта кўп элементлар ўзгаришига олиб келиши алмаштириш босқичлари сонини камайтириш имконини беради.

Қуйидаги 2.15- ва 2.16-мисолларда модуль $n=256$ ҳоли учун киришда *1* тадан элемент ўзгарганда, *8x1*-тартибли диаматрица-устунлар устида параметрли кўпайтириш ва матрица-устунлар устида кўпайтириш натижаларида ўзгарган соҳалар акс этган:

2.15-мисол: Диаматрица-устунни доимий диаматрица-устунга параметрли кўпайтириш ($R_A=40$, $R_{A'}=41$).

A	$\circledR_3$	**B**	≡	**C**
118		151		165
51		251		102
122		3		245
241	$\circledR_3$	14	≡	47
110		221		211
226		121		67
164		101		209
32		124		252

A'	$\circledR_3$	**B**	≡	**C'**
119		151		61
51		251		97
122		3		248
241	$\circledR_3$	14	≡	61
110		221		176
226		121		188
164		101		54
32		124		120

2.16-мисол: Матрица-устунни скалярга кўпайтириш

$$\begin{array}{|c|}\hline A\\\hline 118\\51\\122\\241\\110\\226\\164\\32\\\hline\end{array} * \begin{array}{|c|}\hline c\\\hline 151\\151\\151\\151\\151\\151\\151\\151\\\hline\end{array} \equiv \begin{array}{|c|}\hline \underline{C}\\\hline 154\\21\\246\\39\\226\\78\\188\\224\\\hline\end{array} \qquad \begin{array}{|c|}\hline \underline{A'}\\\hline 119\\51\\122\\241\\110\\226\\164\\32\\\hline\end{array} * \begin{array}{|c|}\hline c\\\hline 151\\151\\151\\151\\151\\151\\151\\151\\\hline\end{array} \equiv \begin{array}{|c|}\hline \underline{C'}\\\hline 49\\21\\246\\39\\226\\78\\188\\224\\\hline\end{array}$$

Мисоллардан кўриниб турибдики, диаматрица-устунини доимий диаматрица-устунга параметрли кўпайтириш натижасида $\underline{A}$ нинг *1* та элементи ўзгарганда $\underline{C'}$ да устуннинг ҳамма элементлари, яъни *8* та, матрицани скаляр кўпайтиришда эса *1* та элемент ўзгарган.

Криптография масалалари учун тенг асосли диаматрица-устунлар ҳам аҳамиятлироқдир.

Таъриф. Агар берилган иккита тенг ўлчамли диаматрица-устунлардан бири иккинчисининг скаляр сонга кўпайтмасига тенг бўлса, бундай диаматрица-устунлар тенг асосли диаматрица-устунлар деб аталади [16].

Қуйидаги 2.17- ва 2.18-мисолларда модуль $n=23$ бўлганда, $3x1$-тартибли бир асосли диаматрица-устунлар $\underline{A}$ ва $\underline{B}$ кўпайтмаси $\underline{C}$ коммутативлик хоссасига эга бўлиши акс этган:

2.17-мисол

$$\begin{array}{|c|}\hline \underline{A}\\\hline 19\\12\\17\\\hline\end{array} \circledR_3 \begin{array}{|c|}\hline \underline{B}\\\hline 7\\2\\22\\\hline\end{array} \equiv \begin{array}{|c|}\hline \underline{C}\\\hline 17\\18\\14\\\hline\end{array}$$

2.18-мисол

$$\begin{array}{|c|}\hline \underline{B}\\\hline 7\\2\\22\\\hline\end{array} \circledR_3 \begin{array}{|c|}\hline \underline{A}\\\hline 19\\12\\17\\\hline\end{array} \equiv \begin{array}{|c|}\hline \underline{C}\\\hline 17\\18\\14\\\hline\end{array}$$

Тенг асосли диаматрица-устунлар учун натижавий параметрли кўпайтма куйидагича (2.22) ифодаланади:

$$x^* \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \circledR_3 y^* \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \equiv z^* \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \qquad (2.22)$$

$$z^* \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \equiv (x+y+x^*R^*y)^* \begin{vmatrix} a_0 \\ a_1 \\ . \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \quad (2.23)$$

Бу ерда $z \equiv x + y + x^* R^* y \ (mod\ n)$.

Диаматрица-устун аслида махсус тузилмали диаматрицанинг тури бўлган содда тузилмали диаматрицанинг бир устунли модели бўлгани сабабли, диаматрица-устуннинг тескариси, транспонирланган диаматрица-устун ва диаматрица-устун диадетерминанти тушунчаларидан фойдаланиш ўринлидир.

Таъриф. $\hat{C}$ — чекли, яъни, n та элементдан иборат бутун сонлар тўплами устида аниқланган mx1 тартибли диаматрица-устунлар тўплами, $\acute{\omega}=\{\circledR_3, 0, ^t, ^{\backslash -1}\}$ — $\hat{C}$ устида аниқланган алгебраик амаллар тўплами бўлса, $(\hat{C};\ \acute{\omega})$ — жуфтлик диаматрица-устунлар алгебраик структураси (қисқача, диаматрица-устунлар алгебраси) деб аталади; бу ерда ўзаро мос тарзда диаматрица-устунлар алгебрасининг $\circledR_3$ — параметрли кўпайтириш, 0 — диаматрица-устунлар алгебрасининг бирлик элементи, ^{t} — транспонирлаш, $^{\backslash -1}$ — параметрли тескарилаш амаллари рамзларидир.

Келтирилган таърифда параметрли вектор кўпайтириш амали учун параметр $R\geq 0$ шартини каноатлантириши назарда тутилгани туфайли, $R=0$ бўлганда, параметрли кўпайтириш амали анъанавий қўшиш амали вазифасини ўтайди.

Берилган диаматрица-устун $\underline{A}$ учун тескари диаматрица-устун $\underline{A}^{\backslash -1}$ билан белгиланади ва $\underline{A}^{\backslash -1}$ диаматрица-устун $\underline{A}$ нинг диадетерминанти Δ нолдан фарқли бўлсагина мавжуд бўлади. Диаматрица-устун $\underline{A}$ учун тескари диаматрица-устун $\underline{A}^{\backslash -1}$ ҳосил қилиш тартиботи бўлимнинг 2.5-бандида келтирилган.

Сатрлар бўйлаб бир устунда $a_0, a_1, a_2, .. a_{m-2}, a_{m-1}$ элементлардан тузилган диаматрица-устун $\underline{A}$ нинг транспонирланган шакли диаматрица-сатр $\underline{A}^t = [a_0\, a_1 a_2 .. a_{m-2} a_{m-1}]^t$ бўлади.

mx1 тартибли диаматрица-устун $\underline{A}$ нинг диадетерминанти Δ куйида келтирилган ифода (2.24) бўйича ҳисобланади:

$$\Delta \equiv (1+ a_0 + a_1 + a_2 + .. a_{m-2} + a_{m-1})^{m-2} \ (mod\ n). \quad (2.24)$$

2.5 Махсус тузилмали диаматрицани ва матрица-устунларни тескарилаш

2-бўлимда таъкидлаб ўтилганидек, диаматрицани тескарилаш натижасида унга тескари бўлган диаматрицани ҳосил қилиш учун, A диадетерминанти 0 дан фарқли бўлса:

$(d_1A)^{\backslash\backslash -1} \equiv d_1((d_1A)^{-1})$ ва $(d_2A)^{\backslash -1} \equiv d_2((d_2A)^{-1})$

ифодаларига монанд ҳисобланади ва бунда

$(d_1A)^{\backslash\backslash -1} \circledR_1 d_1A \equiv E$ ва $(d_2A)^{\backslash -1} \circledR_2 d_2A \equiv E$

тақкосламалари кучга эга бўлади.

Қуйида махсус тузилмали диаматрицалар ва матрица-устунларни тескарилаш жараёнлари ҳақида тўхталамиз.

Берилган махсус тузилмали mxm тартибли диаматрица dA ни модуль n бўйича mxm тартибли $(dA)^{\backslash -1}$ га айлантириш учун қуйидаги амаллар кетма-кетлиги — 2.1-алгоритмни бажариш лозим:

2.1-алгоритм.

1. 2-бўлимда келтирилган (2.14) ифода бўйича dA учун диадетерминант Δ ни ҳисобланг. Агар $\Delta > 0$ бўлса, кейинги қадамга ўтинг; акс ҳолда dA учун тескари диаматрица мавжуд эмас.

2. $\Delta_t \equiv \Delta^{-1} \ (mod\ n)$ ни ҳисобланг.

3. $(dA)^{\backslash -1}$ нинг нодиагонал элементларига мос алгебраик тўлдирувчилар Δ_{ijt} ни ҳисобланг. Бу ерда, агар $i=0$, унда $0<j<m$, агар $0<i<m$, унда $0 \le j < I$. Δ_{ijt} ни ҳисоблаш 2.2-алгоритмда келтирилган.

4. $(dA)^{\backslash -1}$ нинг диагонал элементи a_{IIt} ни ҳисобланг (a_{IIt} ни ҳисоблаш 2.3-алгоритмда келтирилган).

5. $(dA)^{\backslash -1}$ нинг нодиагонал элементлари $a_{ijt} \equiv -\Delta_{ij} * \Delta_t \ (mod\ n)$ ни ҳисобланг.

6. $(dA)^{\backslash -1}$ нинг элементлари асосида махсус тузилмали тескари диаматрицани шакллантиринг.

2.2-алгоритм. Δ_{ijt} ни ҳисоблаш.

1. dA да 1-устунни ўчиринг ва 1-қаторни белгиланг.

2. JJ диагонални нолланг ва нолланмаган диагонал элементларни J қатор элементларига қўшинг.

3. 1-қатор элементларини диагонал элементларга устун бўйлаб кўчиринг ва 1-қаторни ўчиринг.

4. *dA* нинг қолган қисми бўлмиш (*m-1*)х(*m-1*) тартибли диаматрицани шакллантиринг.

5. Агар (*m-1*)х(*m-1*) тартибли диаматрица *I=0* ва *J=1* га тегишли бўлса, унда *2.2* да келтирилган ифода бўйича детерминант Δ_{01} ни ҳисобланг, акс ҳолда қуйида келтирилган *diaminor*( ) функцияси қиймати Δ_{ij} ни ҳисобланг.

diaminor($\{a_{ij}\}$, *p*) функцияси асосида (*m-1*)х(*m-1*) тартибли диаматрица учун диагонал элементлар бўйича ёйиш теоремаси [10, 13] асосида аниқланиши мумкин.

diaminor (a_{00}, a_{10}, a_{20}, a_{01}, a_{11}, a_{21}, a_{02}, a_{12}, a_{22}, *n*) функцияси *3*х*3* тартибли диаматрица учун қуйидаги ифодага эга:

$diaminor() = (a_{00}*((a_{01}+a_{11})*(a_{12}+a_{02}+a_{22})+a_{21}*(a_{02}+a_{22}))+(a_{11}*$
$*(a_{10}*a_{02}+a_{12}+a_{22})+a_{20}*(a_{12}+a_{22}))+(a_{22}*a_{20}*(a_{01}+a_{21})+a_{10}*a_{21}))$
$(mod\ n)$.

2.3-алгоритм. a_{11t} ни ҳисоблаш.

1. *dA* нинг ҳар бир *1*-устун элементини диагонал элемент қийматига қўшиб қўйинг.

2. *dA* нинг *1*-устун ва *1*-қаторини ўчириб, қолган қисми бўлмиш (*m-1*)х(*m-1*) тартибли махсус тузилмали диаматрица учун 2-бўлимда келтирилган (2.14) ифода бўйича диадетерминант Δ_{11} ни ҳисобланг.

3. $a_{11t} \equiv \Delta_t * (\Delta_{01} + \Delta_{11} + \Delta_{21} + .. \Delta_{(m-2)1} + \Delta_{(m-1)1})\ (mod\ n)$ ни ҳисобланг.

Юқорида келтирилган 2.1-алгоритмни *4*х*4* тартибли махсус тузилмали диаматрица *dA* га модуль *n=257* бўлганда қўллаш натижасида унга тескари бўлган *4*х*4* тартибли махсус тузилмали диаматрица $(dA)^{-1}$ ҳосил қилиниб, диаматрицалар *dA* ва $(dA)^{-1}$ ларнинг чапдан ва ўнгдан бир-бирига кўпайтмаси бирлик элементи *E* га тенглиги қуйидаги 2.21-мисолда акс этган:

2.21-мисол

$$\begin{vmatrix} 147 & 47 & 170 & 165 \\ 145 & 147 & 145 & 145 \\ 154 & 145 & 147 & 154 \\ 3 & 120 & 245 & 147 \end{vmatrix}_{(dA)^{-1}} \circledR_2 \begin{vmatrix} 7 & 1 & 2 & 3 \\ 3 & 7 & 3 & 3 \\ 2 & 4 & 7 & 2 \\ 3 & 5 & 6 & 7 \end{vmatrix}_{dA} \equiv \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}_{E}$$

$$\begin{array}{|cccc|} \multicolumn{4}{c}{dA} \\ 7 & 1 & 2 & 3 \\ 3 & 7 & 3 & 3 \\ 2 & 4 & 7 & 2 \\ 3 & 5 & 6 & 7 \end{array} \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{|cccc|} \multicolumn{4}{c}{(dA)^{-1}} \\ 147 & 47 & 170 & 165 \\ 145 & 147 & 145 & 145 \\ 154 & 145 & 147 & 154 \\ 3 & 120 & 245 & 147 \end{array} \equiv \begin{array}{|cccc|} \multicolumn{4}{c}{E} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}$$

Матрица-устунларни тескарилаш учун юқорида келтирилган 2.2-алгоритмни mxm тартибли dA содда тузилмали диаматрица dA га қўллаш кифоя қилади. Натижада mxm тартибли содда тузилмали диаматрица $(dA)^{-1}$ ҳосил бўлади. Бунда содда тузилмали диаматрица dA га тескари бўлган содда тузилмали диаматрица $(dA)^{-1}$ элементлари жуда осон ҳисобланади. Чунки, 2.2-алгоритмининг *1-4* қадамларини ҳамда 2.3-алгоритмнинг *1-2* қадамларини бажариш окибатида ҳар гал диагонал элементлари бир хил бўлиб, нодиагонал элементлари оддий тузилмали диаматрицага хос бўлган диаматрица ҳосил бўлади. Бу эса диаматрицани тескарилаш ифодаларини соддалаштиради.

Қуйидаги 2.22-мисолда модуль n=*257* бўлганда, *4*-тартибли содда тузилмали диаматрицалар dA ва унга тескари бўлган содда тузилмали диаматрица $(dA)^{-1}$ га чапдан ва ўнгдан кўпайтмаси бирлик элементи E га тенглиги акс этган:

2.22-мисол.

$$\begin{array}{|cccc|} \multicolumn{4}{c}{(dA)^{-1}} \\ 1 & 17 & 17 & 17 \\ 154 & 1 & 154 & 154 \\ 34 & 34 & 1 & 34 \\ 171 & 171 & 171 & 1 \end{array} \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{|cccc|} \multicolumn{4}{c}{dA} \\ 1 & 2 & 2 & 2 \\ 3 & 1 & 3 & 3 \\ 4 & 4 & 1 & 4 \\ 5 & 5 & 5 & 1 \end{array} \equiv \begin{array}{|cccc|} \multicolumn{4}{c}{E} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

$$\begin{array}{|cccc|} \multicolumn{4}{c}{dA} \\ 1 & 2 & 2 & 2 \\ 3 & 1 & 3 & 3 \\ 4 & 4 & 1 & 4 \\ 5 & 5 & 5 & 1 \end{array} \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{|cccc|} \multicolumn{4}{c}{(dA)^{-1}} \\ 1 & 17 & 17 & 17 \\ 154 & 1 & 154 & 154 \\ 34 & 34 & 1 & 34 \\ 171 & 171 & 171 & 1 \end{array} \equiv \begin{array}{|cccc|} \multicolumn{4}{c}{E} \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

mx*1*-тартибли a_0, a_1, a_2,.. a_{m-2}, a_{m-1} элементлардан тузилган диаматрица-устун $\underline{A}$ га тескари бўлган диаматрица-устун $\underline{A}^{-1}$

ни шакллантириш учун қуйидаги қадамлар кетма-кетлигини бажариш лозим:

2.4-алгоритм.

1. $R \equiv a_0 + a_1 + a_2 + .. a_{m-2} + a_{m-1} \ (mod\ n)$ ни ҳисобланг. Агар $R = n-1$ бўлса, диаматрица-устун $\underline{A}$ учун тескари диаматрица-устун мавжуд эмас, акс ҳолда кейинги қадамга ўтинг.
2. $R_{+i} \equiv (R+1)^{-1} (mod\ p)$ ни ҳисобланг.
3. $a_{it} \equiv -a_i * R_{+i} \ (mod\ p)$ ни ҳисобланг. Бу ерда $0 \geq i < m$.
4. *3*-қадамда топилган элементлардан $\underline{A}^{\backslash -1}$ ни шакллантиринг.

Қуйидаги 2.23-мисолда модуль $n=257$ бўлганда $4x1$-тартибли диаматрица-устун $\underline{A}$ ва унга тескари бўлган диаматрица-устун $\underline{A}^{\backslash -1}$ га чапдан ва ўнгдан кўпайтмаси ноль элементи *0* га тенглиги акс этган:

2.23-мисол

A		*A\-1*		*0*
2		*17*		*0*
3	$\circledR_3$	*154*	$\equiv$	*0*
4		*34*		*0*
5		*171*		*0*

A\-1		*A*		*0*
17		*2*		*0*
154	$\circledR_3$	*3*	$\equiv$	*0*
34		*4*		*0*
171		*5*		*0*

Қуйидаги 2.24-мисолда модуль $n=256$ бўлганда $8x1$-тартибли дастлабки диаматрица-устун $\underline{H}$ ни ўнгдан шифрлаш калит диаматрица-устуни $\underline{K}$ га кўпайтмаси $\underline{H} \circledR_3 \underline{K}$ ва унинг калит диаматрица-устуни $\underline{K}$ га тескари бўлган диаматрица-устун $\underline{K}^{\backslash -1}$ га кўпайтмаси дастлабки диаматрица-устун $\underline{H}$ га тенглиги акс этган:

2.24-мисол. Шифрлаш-дешифрлаш

$\underline{H}$	$\circledR_3$	$\underline{K}$	$\equiv$	$\underline{H}\circledR_3\underline{K}$	$\circledR_3$	$\underline{K}^{\backslash 1}$	$\equiv$	$\underline{H}$
119		*151*		*61*		*11*		*119*
51		*251*		*97*		*159*		*51*
122		*3*		*248*		*7*		*122*
241	$\circledR_3$	*14*	$\equiv$	*61*	$\circledR_3$	*118*	$\equiv$	*241*
110		*221*		*176*		*89*		*110*
226		*121*		*188*		*197*		*226*
164		*101*		*54*		*65*		*164*
32		*124*		*120*		*204*		*32*

Бу ерда $\underline{K}^{\setminus -1}$ учун $R_{+t} \equiv (R+1)^{-1} (mod\ 256) \equiv 83$.

Келтирилган мисолдан диаматрица-устунлар алгебрасидан шифрлаш ва хэшлаш алгоритмларини яратишда фойдаланиш мумкинлиги кўриниб турибди. Бу алгебранинг қулайлиги диаматрица-устунларни тескарилаш осонлиги ва диаматрица-устунни доимий диаматрица-устунга параметрли кўпайтириш натижасида дастлабки диаматрица-устуннинг битта элементи ўзгарганда, натижавий диаматрица-устунда ҳамма элементлар ўзгариши ҳодисаси билан исботланади.

2.6 Бутун сонли ва матрицавий параметрли алгебраик структуралар

Қуйида криптографик тизимлар яратишга мўлжалланган бутун сонли ва матрицавий параметрли алгебраик структураларни шакллантириш асослари баён этилган. Бундай алгебраик структуралар асосида мавжуд криптоалгоритмларга аналог алгоритмлар яратиш усулидан [19-21] фойдаланиш, криптомодуллар тезлигини ва криптобардошлилигини ошириш имконини беради.

Элементлари бир хил a ва b лардан таркиб топган икки mx1 тартибли диаматрица-устун

$$\underline{A} = \begin{vmatrix} a \\ a \\ . \\ a \end{vmatrix} \quad \text{ва} \quad \underline{B} = \begin{vmatrix} b \\ b \\ . \\ b \end{vmatrix}$$

устида параметрли кўпайтириш амали қуйидаги кўринишида ифодаланиб,

$$a^* \begin{vmatrix} 1 \\ 1 \\ . \\ 1 \end{vmatrix} \circledR_3\ b^* \begin{vmatrix} 1 \\ 1 \\ . \\ 1 \end{vmatrix} \equiv (a+b+a^*R^*b)^* \begin{vmatrix} 1 \\ 1 \\ . \\ 1 \end{vmatrix}$$

унда кўпайтувчилар a ва b ҳамда параметр $R \equiv m(mod\ n)$ скалярлардир. Мазкур ифодада m та бирдан таркиб топган диаматрица-устун ташувчи ахборот параметр R да мужассамланганлиги туфайли, информативлик нуқтаи назаридан бу ифода ҳақида ахборот

$$a®b \equiv a + b + a*R*b\ (mod\ n) \qquad (2.25)$$

ифодасида мужассамдир. Шуни эътиборга олиб, чекли, яъни n та элементдан иборат бутун сонлар тўплами устида $a®b \equiv a+b+a*R*b\ (mod\ n)$ ифодаси асосида кўпайтириш амалини аниқлаш мумкин. Бу амал тернар бўлиб, параметрли кўпайтириш амали деб аталади ва ® рамзи билан белгиланади. Параметрли кўпайтириш амали берилган тўпламда нолдан фарқли тўплам элементи a учун тескари элемент $a^{\backslash -1}$ ва қарама-карши элемент n -a мавжуд. $a^{\backslash -1}$ параметрли тескари элемент деб аталади ва $a®\ a^{\backslash -1} \equiv 0\ (mod\ n)$ шартини қаноатлантиради. Бу ерда 0 — параметрли бирлик элементи бўлиб, $a®0 \equiv a$ аксиомани қаноатлантиради. Параметрли тескари элемент қуйидагича ҳисобланади:

$$a^{\backslash -1} \equiv - a*(1+ a\ * R)^{-1}\ (mod\ n) \qquad (2.26)$$

Бу ерда $^{-1}$ — n модуль бўйича тескарилаш амалининг рамзидир.

Юқорида келтирилган амаллар асосида тузилган алгебраик структурага қуйидаги таърифни берамиз.

Таъриф. F_n — чекли, яъни n та элементдан иборат бутун сонлар тўплами, параметр $R \in F_n$ бўлса, $\Omega=\{®,\ ®_0,\ 0,^{\backslash -1}\}$ — F_n устида аниқланган алгебраик амаллар тўплами бўлса, $(F_n; \Omega)$ — жуфтлик параметрли алгебраик структура (қисқача, параметрли алгебра) деб аталади; бу ерда ўзаро мос тарзда ® — параметрли алгебранинг $R>0$ параметрли кўпайтириш, $®_0$ — $R=0$ параметрли кўпайтириш, 0 — бирлик элементининг, $^{\backslash -1}$ — параметрли тескарилаш амалларининг рамзларидир.

Қуйида модуль $n=257$ бўлганда бутун сонларнинг параметрга чапдан ва ўнгдан параметрли кўпайтмаси коммутативлиги акс этган:

a	*R*	*b*		*a®b*
97	*101*	*131*	≡	*177*
b	*R*	*a*		*a®b*
131	*101*	*97*	≡	*177*

Юқорида келтирилганлардан кўриниб турибдики, бутун сонли параметрли алгебранинг асосий амали бўлган параметрли кўпайтириш амали элементлари бир хил *a* ва *b* лардан таркиб топган иккита *mx1* тартибли диаматрица-устунлар *A, B* устида кўпайтириш амали асосида шаклланган. Мазкур алгебранинг бирлик элементи *0* га тенг.

Таъриф. Параметрли алгебра $(F_n; \Omega)$ да фақат битта параметр $R>0$ аниқланган бўлса, $(F_n; ®, 0, ^{-1})$ тўртлик параметрли алгебранинг ***параметрли коммутатив группаси*** деб аталади; бу ерда ўзаро мос тарзда F_n — n элементли бутун сонлар тўплами, ® — параметрли алгебранинг $R>0$ параметрли кўпайтириш, *0* — бирлик элементининг, $^{-1}$ — параметрли тескарилаш амалларининг рамзларидир.

Коммутатив группанинг барча аксиомалари [7] параметрли алгебрани ҳам қаноатлантиради:

$\forall a,b,c \in F_n: a®b \equiv c \ (mod\ n)$ (*ёпиқлик аксиомаси*). (1)

$\forall a,b,c \in F_n: (a®b)® c \equiv a®(b® c) \ (mod\ n)$ (*ассоциативлик аксиомаси*). (2)

$\forall a \in F_n \exists e=0: a® e \equiv a \ (mod\ n)$ (*айният аксиомаси*). (3)

$\forall a \neq 0 \in F_n \exists a^{-1}: a ® a^{-1} \equiv e \ (mod\ n)$ (*тескари элемент мавжудлиги — инверсия аксиомаси*). (4)

$\forall a,b \in F_n: a®b \equiv b ® a \ (mod\ n)$ (*коммутативлик аксиомаси*).(5)

Шуни таъкидлаш жоизки, параметрли кўпайтириш амали параметр $R>0$ бўлса, тўла маънода параметрли кўпайтириш амали вазифасида, $R=0$ бўлса анъанавий кўшиш амали вазифасида талқин этилади. $R=0$ бўлганда параметрли кўпайтириш амали $®_0$ билан белгиланади. Бундай белгилаш параметрли алгебра тушунчасининг майдон тушунчасига муносабатини изоҳлашда аҳамиятга эга.

Параметр $R>0$ бўлса, ***параметрли коммутатив группа мультипликатив,*** параметр $R=0$ бўлса, ***параметрли коммутатив группа аддитивдир.***

Параметрли мультипликатив коммутатив группа қуйидаги хоссаларга эга.

1-хосса: агар параметрли мультипликатив коммутатив группанинг параметри жуфт сон ва модули $n=2^k$ (k — ихтиёрий натурал сон) га тенг бўлса, унинг тартиби (группа элементлари сони) 2^k га тенг.

2-хосса: агар модули n туб сон бўлган параметрли мультипликатив коммутатив группанинг параметри ихтиёрий натурал сон бўлса, унинг тартиби $\varphi(n)$ га тенг, бу ерда $\varphi(n)$ — Эйлер пи-функцияси қиймати.

Мисол:

1) $(F_8; ®, 0, ^{-1})$, бу ерда $F_8=\{0,1,2,3,4,5,6,7\}$, $n=2^3$, $R=2$.

2) $(F_{\varphi(7)}; ®, 0, ^{-1})$, бу ерда $F_7=\{0,1,2,3, 5,6\}$, $n=7$, $R=5$.

Бу алгебраларда F_n нинг барча элементлари учун коммутатив группа аксиомалари қаноатлантирилади. Қуйида келтирилган жадвалда 1- ва 2-хоссалар учун F_n нинг барча нолдан фарқли элементларининг мавжуд параметрли тескари элементлари келтирилган.

2.1-жадвал

n	***R***	*1*	*2*	*3*	*4*	*5*	*6*	*7*
8	*2*	*5*	*6*	*3*	*4*	*1*	*2*	*7*
7	*5*	*1*	*3*	*2*	*м.э*	*6*	*5*	

Бу ерда *м.э.* F_n нинг мазкур элементи учун параметрли тескари элементи мавжуд эмаслигини билдиради.

3-хосса: агар мураккаб модулли параметрли мультипликатив коммутатив группанинг параметри модуль n билан ўзаро туб бўлса, унинг тартиби $\varphi(n)$ га тенг, бу ерда $\varphi(n)$ — Эйлер пи-функцияси қиймати.

4-хосса: агар мураккаб модуль $n=p*q$, бу ерда p, q — ҳар хил туб сонлар, параметрли мультипликатив коммутатив груп-

панинг параметри R модуль p билан ўзаро туб бўлиб, q билан ўзаро туб бўлмаса, унинг тартиби $p*(q-1)$ га тенг.

Қуйида келтирилган жадвалда 3- ва 4-хоссалар учун F_n нинг барча нолдан фарқли элементларининг мавжуд параметрли тескари элементлари келтирилган.

2.2-жадвал

n	*R*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*
35	*4*	*м.э.*	*27*	*24*	*8*	*м.э.*	*м.э.*	*7*	*4*	*13*	*10*	*м.э.*	*м.э.*	*9*	*28*	*25*	*м.э.*	*17*
35	*14*	*м.э.*	*12*	*4*	*3*	*30*	*м.э.*	*7*	*34*	*33*	*25*	*м.э.*	*2*	*29*	*28*	*20*	*м.э.*	*32*

18	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*	*32*	*33*	*34*
29	*м.э.*	*30*	*м.э.*	*32*	*34*	*3*	*15*	*м.э.*	*2*	*14*	*18*	*20*	*м.э.*	*22*	*м.э.*	*23*
24	*23*	*15*	*м.э.*	*27*	*19*	*18*	*10*	*м.э.*	*22*	*14*	*13*	*5*	*м.э.*	*17*	*9*	*8*

Келтирилган мисоллардан, модуль $n=35$ бўлганда, параметр $R=4$ бўлса, параметрли мультипликатив коммутатив группа $(F_{\varphi(35)}; \circledR, 0, ^{-1})$ нинг элементлари тўплами $F_{\varphi(35)}=\{0, 2, 3, 4, 5, 7, 8, 9, 10, 13, 14, 15, 17, 18, 20, 22, 23, 24, 25, 27, 28, 29, 30, 32, 34\}$ параметр $R=14$ бўлса, параметрли мультипликатив коммутатив группа $(F_{7*(5-1)}; \circledR, 0, ^{-1})$ нинг элементлари тўплами $F_{7*(5-1)}=\{0, 2, 3, 4, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 25, 27, 28, 29, 30, 32, 33, 34\}$, яъни $R=4$ ҳолига нисбатан 4 та ортиқ экани аён бўлади.

Параметрлари $R>0$ ва $R=0$ бўлган параметрли алгебрада тўплам бирлик ва 0 элементлари учун ва дистрибутивлик хоссасига оид аксиомадан бошқа барча ***анъанавий майдон*** ва ***коммутатив группага оид*** (1)-(5) аксиомалар қаноатлантирилади. Бунда алгебра тартиби (алгебра элементлари сони) n га тенг ёки ундан кичик ($\varphi(n)$ ёки $(p*(q-1))$ бўлиши мумкин.

Параметрли алгебрада $\forall a \in F_n \exists\, 0=0 : a \circledR_0 0 \equiv a \,(mod\, n)$ (*айният аксиомаси*) (*6*) ва $\forall a \in F_n \exists\, (-a) : a \circledR_0 (-a) \equiv 0 \,(mod\, n)$ (*қарама-қарши элемент мавжудлиги аксиомаси*) (*7*) *қаноатлантирилса*

ҳам, майдоннинг бирлик ва ноль элементлари фарқли бўлиши зарурлиги ҳақидаги шарт [7] қаноатлантирилмайди.

Параметрли алгебрада

$\forall a, b, c \in F_n : (a®_0 b)®c \equiv (a®c) ®_0 (b®c) \ (mod\ p)$ (8) кўринишдаги *дистрибутивлик аксиомаси* қаноатлантирилмайди. Бинобарин, параметрли алгебра майдон ҳам, ҳалқа ҳам эмас.

Қуйида модуль $p=257$, $R=11$, $a=6$ учун *1-8* аксиомаларга мисоллар келтирилган.

Мисол:

Тартиб рақами	***b***	***c***	***е ёки 0***	a^{-1}	***-a***	***чап***	***ўнг***
1	*17*	*117*				*117*	
2	*17*	*201*				*206*	*206*
3			*0*			*6*	*6*
4				*138*		*0*	
5	*17*					*117*	*117*
(6)			*0*			*6*	*6*
(7)					*251*	*0*	*6*
(8)	*17*	*201*				*191*	*135*

Параметрли мультипликатив коммутатив группанинг *1-*, *2-*, *4-*хоссалари ***анъанавий мультипликатив группа*** $(F_n; *, 1, ^{-1})$ ***хоссаларидан ўз тартиби*** билан фарқ қилади. Масалан, анъанавий бинар кўпайтириш амали асосида шаклланган мультипликатив группа модули 2^k бўлганда, фақат тоқ элементлардан ташкил топган чекли тўпламда мавжуд бўлса, параметрли мультипликатив коммутатив группа бутун сонлар тўпламида мавжуддир. Мураккаб модуль $n=p*q$ учун параметрли мультипликатив коммутатив группанинг параметри R модуль p билан ўзаро туб бўлиб, q билан ўзаро туб бўлмаса унинг ***тартиби анъанавий мультипликатив группа*** $(F_n; *, 1, ^{-1})$ ***тартибига нисбатан юқори*** бўлади. Булар криптотизим яратишнинг янги имкониятларини юзага чиқаради.

Агар a®b ифодаси mxm тартибли матрицалар учун матрицалар алгебрасида ёзилса, у қуйидаги кўринишга эга бўлади.

$$\underset{A}{\begin{vmatrix} a_{00} & a_{01} & a_{02} & \dots & a_{0(m-2)} & a_{0(m-1)} \\ a_{10} & a_{11} & a_{12} & \dots & a_{1(m-2)} & a_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{(m-2)0} & a_{(m-2)1} & a_{(m-2)2} & \dots & a_{(m-2)(m-2)} & a_{(m-2)(m-1)} \\ a_{(m-1)0} & a_{(m-1)1} & a_{(m-1)2} & \dots & a_{(m-1)(m-2)} & a_{(m-1)(m-1)} \end{vmatrix}} \underline{\text{®}} \underset{B}{\begin{vmatrix} b_{00} & b_{01} & b_{02} & \dots & b_{0(m-2)} & b_{0(m-1)} \\ b_{10} & b_{11} & b_{12} & \dots & b_{1(m-2)} & b_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ b_{(m-2)0} & b_{(m-2)1} & b_{(m-2)2} & \dots & b_{(m-2)(m-2)} & b_{(m-2)(m-1)} \\ b_{(m-1)0} & b_{(m-1)1} & b_{(m-1)2} & \dots & b_{(m-1)(m-2)} & b_{(m-1)(m-1)} \end{vmatrix}} \equiv$$

$$\equiv \underset{A+B}{\begin{vmatrix} a_{00}+b_{00} & a_{01}+b_{01} & \dots & a_{0(m-2)}+b_{0(m-2)} & a_{0(m-1)}+b_{0(m-1)} \\ a_{10}+b_{10} & a_{11}+b_{11} & \dots & a_{1(m-2)}+b_{1(m-2)} & a_{1(m-1)}+b_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots \\ a_{(m-2)0}+b_{(m-2)0} & a_{(m-2)1}+b_{(m-2)1} & \dots & a_{(m-2)(m-2)}+b_{(m-2)(m-2)} & a_{(m-2)(m-1)}+b_{(m-2)(m-1)} \\ a_{(m-1)0}+b_{(m-1)0} & a_{(m-1)1}+b_{(m-1)1} & \dots & a_{(m-1)(m-2)}+b_{(m-1)(m-2)} & a_{(m-1)(m-1)}+b_{(m-1)(m-1)} \end{vmatrix}} + \underset{A}{\begin{vmatrix} a_{00} & a_{01} & \dots & a_{0(m-2)} & a_{0(m-1)} \\ a_{10} & a_{11} & \dots & a_{1(m-2)} & a_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots \\ a_{(m-2)0} & a_{(m-2)1} & \dots & a_{(m-2)(m-2)} & a_{(m-2)(m-1)} \\ a_{(m-1)0} & a_{(m-1)1} & \dots & a_{(m-1)(m-2)} & a_{(m-1)(m-1)} \end{vmatrix}} \text{x}$$

$$\text{x} \underset{R}{\begin{vmatrix} R_{00} & R_{01} & \dots & R_{0(m-2)} & R_{0(m-12)} \\ R_{10} & R_{11} & \dots & R_{1(m-2)} & R_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots \\ R_{(m-2)0} & R_{(m-2)1} & \dots & R_{(m-2)(m-2)} & R_{(m-2)(m-1)} \\ R_{(m-1)0} & R_{(m-1)1} & \dots & R_{(m-1)(m-2)} & R_{(m-1)(m-1)} \end{vmatrix}} \text{x} \underset{B}{\begin{vmatrix} b_{00} & b_{01} & \dots & b_{0(m-2)} & b_{0(m-1)} \\ b_{10} & b_{11} & \dots & b_{1(m-2)} & b_{1(m-1)} \\ \dots & \dots & \dots & \dots & \dots \\ b_{(m-2)0} & b_{(m-2)1} & \dots & b_{(m-2)(m-2)} & b_{(m-2)(m-1)} \\ b_{(m-1)0} & b_{(m-1)1} & \dots & b_{(m-1)(m-2)} & b_{(m-1)(m-1)} \end{vmatrix}}$$

Бу ерда + ва x анъанавий матрицалар алгебрасининг модуль арифметикасида матрицалар устида берилган қўшиш ва кўпайтириш амаллари рамзларидир. A, $\underline{R}$, B матрицалари устида аниқланган кўпайтириш амали тернар бўлиб, остки чизиқли $\underline{\text{®}}$ рамзи билан белгиланади ва матрицавий параметрли кўпайтириш амали деб аталади.

Матрицавий параметрли тескарилаш амали қуйидаги ифода бўйича ҳисобланади:

$A^{\backslash -1} \equiv - A\text{x}(E+A\text{x}\underline{R})^{-1} (mod\ n)$

Бу ерда $^{-1}$ — матрицавий тескарилаш, E — бирлик матрицаси рамзларидир. Матрицавий параметрли тескари матрица $A^{\backslash -1}$ ни ҳисоблаш A матрица элементларининг қарама-қарши қийматларидан тузилган матрица — A ни шакллантириш, $(E+A\text{x}\underline{R})$ $(mod\ n)$ ни ҳисоблаш, $(E+A\text{x}\underline{R})$ га тескари матри-

ца $(E+A\underline{R})^{-1}$ ни ҳисоблаш ва уни чапдан — A га матрицавий кўпайтириш амалларини ўз ичига олади.

Берилган A матрицага матрицавий параметрли тескари матрица $A^{\backslash -1}$

$$A\ \underline{®}A^{\backslash -1} \equiv 0\ (mod\ n)$$

аксиомани қаноатлантиради. Бу ерда 0 — 0 элементлардан шаклланган бирлик матрицаси бўлиб,

$$A\ \underline{®}0 \equiv A\ (mod\ n)$$

аксиомани қаноатлантиради.

Юқорида келтирилган амаллар асосида тузилган алгебраик структурага қуйидаги таърифни берамиз.

Таъриф. $\underline{Ď}$ — чекли, яъни n та элементдан иборат бутун сонлар тўплами устида аниқланган квадрат матрицалар тўплами, матрицавий параметр $\underline{R} \in \underline{Ď}$, $\underline{Ω} = \{ \underline{®}, \underline{®}_0, 0, {}^{t}, {}^{\backslash -1} \}$ — $\underline{Ď}$ устида аниқланган алгебраик амаллар тўплами бўлса, $(\underline{Ď}; \underline{Ω})$ — жуфтлик матрицавий параметрли алгебраик структура (қисқача, матрицавий параметрли алгебра) деб аталади; бу ерда ўзаро мос тарзда $\underline{®}$ — матрицавий параметр $\underline{R} \neq 0$ билан кўпайтириш, $\underline{®}_0$ — матрицавий параметр $\underline{R}=0$ билан кўпайтириш, ^{t} — транспонирлаш, $^{\backslash -1}$ — матрицавий параметрли тескарилаш амалларининг, 0 — параметрли бирлик матрицасининг рамзларидир.

Бу ерда транспонирлаш амали анъанавий матрицалар алгебрасининг [10, 101] тушунчасига айнандир.

Мазкур китобда, асосан матрицавий параметрли алгебранинг мультипликатив группаси $(\underline{Ď}; \underline{®}, 0, {}^{t}, {}^{\backslash -1})$ дан фойдаланилган.

Қуйида модуль $n=257$ бўлганда, 4x4-тартибли матрицаларнинг матрицавий параметрга чапдан ва ўнгдан матрицавий параметрли кўпайтмаси нокоммутативлиги акс этган:

A	$\underline{R}$	B		$A\underline{®}B$
178 250 246 242	40 44 48 52	15 256 255 254		155 100 196 167
175 34 245 241	41 45 49 53	254 17 254 254	$\Rightarrow$	195 118 93 36
38 248 50 240	42 46 50 54	255 253 18 255		87 205 97 60
120 247 243 66	43 47 51 55	254 252 251 15		249 172 154 253

$$\begin{array}{cccc} B & \underline{R} & A & B \,\underline{\circledR}\, A \\ \left|\begin{array}{cccc} 15 & 256 & 255 & 254 \\ 254 & 17 & 254 & 254 \\ 255 & 253 & 18 & 255 \\ 254 & 252 & 251 & 15 \end{array}\right| & \left|\begin{array}{cccc} 40 & 44 & 48 & 52 \\ 41 & 45 & 49 & 53 \\ 42 & 46 & 50 & 54 \\ 43 & 47 & 51 & 55 \end{array}\right| & \left|\begin{array}{cccc} 178 & 250 & 246 & 242 \\ 175 & 34 & 245 & 241 \\ 38 & 248 & 50 & 240 \\ 120 & 247 & 243 & 66 \end{array}\right| \Rightarrow & \left|\begin{array}{cccc} 77 & 200 & 230 & 230 \\ 254 & 123 & 246 & 233 \\ 68 & 8 & 250 & 205 \\ 44 & 216 & 20 & 98 \end{array}\right| \end{array}$$

Қуйида модуль $n=257$ ва $\underline{R} = E$ бўлганда, 4x4-тартибли матрица A га матрицавий параметрли тескари матрица $A^{\backslash -1}$ ни ҳосил қилиш жараёни ва A, $A^{\backslash -1}$ матрицалари учун $A \,\underline{\circledR}\, A^{\backslash -1} \equiv 0 \ (mod\ n)$ аксиома қаноатлантирилиши акс этган.

$$\begin{array}{ccccccccccccc} -A & \text{x} & (E & + & A & \text{x} & \underline{R})^{-1} & \equiv & A^{\backslash -1} \\ \left|\begin{array}{cccc} 243 & 1 & 2 & 3 \\ 3 & 241 & 3 & 3 \\ 2 & 4 & 240 & 2 \\ 3 & 5 & 6 & 243 \end{array}\right| & \text{x}(& \left|\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right| & + & \left|\begin{array}{cccc} 14 & 256 & 255 & 254 \\ 254 & 16 & 254 & 254 \\ 255 & 253 & 17 & 255 \\ 254 & 252 & 251 & 14 \end{array}\right| & \text{x} & \left|\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right| &)^{-1} \equiv & \left|\begin{array}{cccc} 191 & 210 & 87 & 92 \\ 112 & 201 & 112 & 112 \\ 103 & 112 & 192 & 103 \\ 254 & 137 & 12 & 96 \end{array}\right| \end{array}$$

$$\begin{array}{ccccc} A & & A^{\backslash -1} & & 0 \\ \left|\begin{array}{cccc} 14 & 256 & 255 & 254 \\ 254 & 16 & 254 & 254 \\ 255 & 253 & 17 & 255 \\ 254 & 252 & 251 & 14 \end{array}\right| & \circledR & \left|\begin{array}{cccc} 191 & 210 & 87 & 92 \\ 112 & 201 & 112 & 112 \\ 103 & 112 & 192 & 103 \\ 254 & 137 & 12 & 96 \end{array}\right| & \equiv & \left|\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right| \end{array}$$

Шундай қилиб, матрицавий параметрли алгебранинг асосий амали бўлган матрицавий параметрли кўпайтириш амали элементлари квадрат шаклли A, B ва $\underline{R}$ матрицалар устида тернар матрицавий кўпайтириш амали асосида шаклланган ва мазкур алгебранинг бирлик элементи ноль-матрицага тенгдир.

2-бўлим бўйича хулосалар

1. Такомиллашган диаматрицалар алгебраси, диаматрица-устунлар алгебраик структураси, бутун сонли ва матрицавий параметрли алгебраик структуралар ишлаб чиқилди ҳамда

улар асосида бажариладиган асосий амаллар ёритиб берилди. Криптография масалаларини ечишда махсус тузилмали диаматрицалардан фойдаланиш, уларни тескарилаш амали соддалиги туфайли, қулайликлар туғдиради.

2. Шифрлар яратишда анъанавий матрицалар алгебраси ўрнига ёки биргаликда такомиллашган диаматрицалар алгебрасидан фойдаланиш мумкин. Бунга кириш диаматрицасини доимий диаматрицага диаматрицавий кўпайтиришга асосланган шифралмаштиришларда киришда битта элемент ўзгариши чиқишда матрицавий кўпайтма чиқишидагига нисбатан *1,5-1,75* марта кўп элементлар ўзгаришига олиб келиши асос бўлади. Бу хосса шифрлаш босқичлари сонини камайтиришга, бинобарин, шифрлаш тезлигини оширишга ёки босқичлар сони ўзгармай колса, криптобардошлиликни оширишга хизмат килади.

3. Шифрлар яратишда анъанавий матрица-устунларга нисбатан диаматрица-устунлардан фойдаланиш эффективдир. Кириш диаматрица-устунини доимий диаматрица-устунга параметрли кўпайтиришга асосланган шифралмаштиришларда киришда битта элемент ўзгариши чиқишда матрицани скаляр кўпайтириш чиқишидагига нисбатан (*m-1*) марта кўп элементлар ўзгаришига олиб келиши алмаштириш босқичлари сонини камайтириш имконини беради

4. Матрицавий параметрли алгебранинг асосий амали бўлган матрицавий параметрли кўпайтириш амали элементлари квадрат шаклли *A, B* ва $\underline{R}$ матрицалар устида тернар матрицавий кўпайтириш амали асосида шаклланган ва мазкур алгебранинг бирлик элементи ноль-матрицага тенгдир.

5. Такомиллашган диаматрицалар, диаматрица-устунлар алгебралари ва бутун сонли ҳамда матрицавий параметрли алгебралардан фойдаланиш мавжуд криптотизимларни такомиллаштириш, уларнинг криптобардошлилигини ошириш, янги криптоалгоритм ва протоколлар яратиш нуқтаи назаридан аҳамиятга моликдир.

7. Параметрли мультипликатив коммутатив группа — параметрли алгебранинг хоссалари анъанавий бинар кўпайтириш

амали асосида шаклланган мультипликатив группа (F_n; *, 1 , $^{-1}$) хоссаларидан ўз тартиби билан фарқ қилади. Анъанавий мультипликатив группа модули 2^k бўлганда фақат тоқ элементлардан ташкил топган чекли тўпламда мавжуд бўлса, параметрли мультипликатив коммутатив группа бутун сонлар тўпламида мавжуддир. Мураккаб модуль $n=p*q$ учун параметрли мультипликатив коммутатив группанинг параметри R модуль p билан ўзаро туб бўлиб, q билан ўзаро туб бўлмаса унинг тартиби анъанавий мультипликатив группа тартибига нисбатан юқори бўлади. Булар криптотизим яратишда янги имкониятларга йўл очади.

3-БЎЛИМ

ДИАМАТРИЦА-УСТУНЛАР АЛГЕБРАСИ ВА ПАРАМЕТРЛИ АЛГЕБРАЛАРГА АСОСЛАНГАН БИР ТОМОНЛАМА КРИПТОГРАФИК ФУНКЦИЯЛАР

3.1 Диаматрица-устунлар алгебраси ва параметрли алгебрада дискрет даражага ошириш

Диаматрица-устунни ўзига параметрли кўпайтириш, яъни квадратлаш натижасида дастлабки диаматрица-устун билан тенг асосли диаматрица-устун ҳосил бўлади. Бинобарин, ҳар қандай диаматрица-устунни бирор дискрет даражага ошириш натижасида агар натижа *0* дан фарқли бўлса, унинг асоси ўзгармайди, яъни дастлабки диаматрица-устунни бирор скаляр сонга кўпайтмаси ҳосил бўлади [16].

Қуйидаги 3.1-мисолда модуль *23* бўйича *3x1* тартибли сатрлар бўйлаб бир устунда *19, 9, 13* элементлардан тузилган ва параметри *R=18* бўлган дастлабки диаматрица-устун $\underline{A}$ учун даража кўрсаткичлари, дастлабки диаматрица-устуннинг скаляр кўпайтувчилари ва даражалар қийматлари парчаси келтирилган.

3.1-мисол.

Даража кўрсаткичи	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	.	.	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*
Скаляр кўпайтувчи	*1*	*20*	*13*	*18*	*21*	*9*	*11*	*3*	.	.	*7*	*19*	*17*	*2*	*16*	*6*	*0*	*1*
Даражалар қийматлари	*19*	*12*	*17*	*20*	*8*	*10*	*2*	*11*	.	.	*18*	*16*	*1*	*15*	*5*	*22*	*0*	*19*
	9	*19*	*2*	*1*	*5*	*12*	*7*	*4*	.	.	*17*	*10*	*15*	*18*	*6*	*8*	*0*	*9*
	13	*7*	*8*	*4*	*20*	*2*	*5*	*16*	.	.	*22*	*17*	*14*	*3*	*1*	*9*	*0*	*13*

Модуль арифметикасида R параметр билан берилган диаматрица-устун $\underline{A}$ нинг даража кўрсаткичи e га тенг бўлган дискрет даражага ошириш натижаси $\underline{C}$ қуйидагича ифодаланади:

$$\left(\begin{vmatrix} \underline{A}^{\backslash e} \\ a_0 \\ a_1 \\ \dots \\ a_{m-2} \\ a_{m-1} \end{vmatrix}\right)^{\backslash e} \equiv (1^{\backslash e})^* \begin{vmatrix} \underline{C} \\ a_0 \\ a_1 \\ \dots \\ a_{m-2} \\ a_{m-1} \end{vmatrix} \quad (3.1)$$

Бу ерда берилган диаматрица-устун $\underline{A}$ учун

$R \equiv a_0 + a_1 + a_2 + .. a_{m-2} + a_{m-1} \ (mod\ n)$,

натижавий диаматрица-устун $\underline{C}$ учун $R_c \equiv R * 1^{\backslash e} \ (mod\ n)$.

R параметр билан дискрет даражага оширишда худди анъанавий дискрет даражага ошириш жараёни каби $1^{\backslash e}$ e ни 2 нинг даража қийматларини ўз ичига олган ва унга тенг бўлган йиғинди кўринишига келтирилиб, рекурсив тарзда ҳисоблашлар орқали амалга оширилади.

Масалан, 1 нинг $e=37$ R параметрли даражаси қуйидагича ҳисобланади:

$$1^{\backslash 37} = 1^{\backslash 32+4+1} \equiv (((((1^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR (1^{\backslash 2})^{\backslash 2}) \circledR 1 (mod\ n),$$

бу ерда $1^{\backslash 2} \equiv 2 + R (mod\ n)$.

Шуни таъкидлаш лозимки, диаматрица-устунни параметрли дискрет даражага ошириш функцияси бир томонлама функция бўлиб, у носимметрик криптотизимлар яратишда аҳамиятга молик.

Параметр R диаматрица-устунлар алгебрасида берилган бир элементли диаматрица-устун элементига тенг бўлса, параметрли алгебрада R — ихтиёрий бутун сондир. Шу боис диаматрица-устунлар алгебрасида 1 ни параметрли дискрет даражага ошириш функцияси, параметрли алгебрада эса дискрет даражага ошириш функциясининг хусусий ҳоли деб қараш ўринлидир.

Параметрли алгебрада a асоснинг e — даражаси $a^{\backslash e}$ билан белгиланади. Бу ерда $^{\backslash e}$ — параметрли e — дискрет даражага ошириш амалининг рамзидир.

Масалан, a нинг $e=37$ R параметрли даражаси қуйидагича ҳисобланади:

$$a^{\backslash 37} = a^{\backslash 32+4+1} \equiv (((((a^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2} \circledR (a^{\backslash 2})^{\backslash 2}) \circledR a \ (mod\ n),$$

бу ерда $a^{\backslash 2} \equiv 2 * a + R * a^2 \ (mod\ n)$

Қуйидаги 3.2-мисолда модуль *23* бўйича *a=19* нинг *R =18* параметрли даража қийматлари парчаси келтирилган.

3.2-мисол

Даража кўрсаткичи	*1*	*2*	*3*	*4*	*5*	*6*	.	.	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*
Даража қийматлари	*19*	*4*	*11*	*20*	*2*	*15*	.	.	*1*	*17*	*8*	*3*	*13*	*16*	*10*	*22*	*21*	*0*	*19*

Кейинги бандда бутун сонли параметрли алгебрада дискрет даражага ошириш функциясининг хоссалари баён этилган.

3.2 Бир томонлама параметрли функциянинг хоссалари

Ошкора криптографияга [87] оид носимметрик криптотизимларни яратиш битта махфийликка эга бўлган бир томонлама функциялардан фойдаланишга асосланади. Энг машҳур носимметрик криптотизимлар, уларнинг асосий характеристикаси бўлган криптобардошлилик дискрет логарифм, эллиптик эгри чизиқли дискрет логарифм ва факторлаштириш масалаларини ечиш асосида махфийликни топишнинг мураккаблигига асосланади. Бунда мураккаблик даражаси криптотизимдан ноқонуний (хакер) ва қонуний фойдаланувчилар учун бир хил бўлиб, катта хисоблаш ресурсига эга ташқи ноқонуний бузғунчилар учун криптотизимни қўпориш хавфига ўрин қолдиради. Қуйида ноқонуний бузғунчиларнинг қўпорувчилик имкониятларини йўққа чиқаришга имкон берувчи, фақат қонуний фойдаланувчилар учунгина маълум бўлган анъанавий махфийликка (даража кўрсаткичи — дискрет логарифм учун, туб кўпайтувчи — факторлаш учун) қўшимча *R* параметрли бир томонлама функциянинг хоссалари баён қилинган [19-21].

Таъриф. Модуль арифметикасида параметр *R≥1* билан даражага ошириш функцияси параметрли функция деб аталади.

Мазкур китобда асосан *2* хил модуль $n \in \{p, p_1 * p_2\}$ бўйича аниқланган параметрли функциянинг хоссалари баён қилинган. Бу ерда p — туб сон, p_1, p_2 — ҳар хил туб сонлар, R — параметр. Модуль n бўйича асос a ни R параметрли x даражага ошириш

натижаси $a^{\backslash x}(mod\ n)$ шаклида ифодаланган, бу ерда $x \in \{0,1,-1,e, d, z\}$, $\backslash$ — R параметрли даражага ошириш рамзидир.

Параметрли функциянинг хоссалари 2 та белги асосида 2 синфга бўлинган: булар анъанавий даражага ошириш функциясига ўхшаш (1-синф) ва фарқли (2-синф) хоссалар бўлиб, ўз навбатида мазкур синфларга оид хоссалар муаллиф томонидан фойдаланишга мўлжалланганига қараб, криптографик тизимлар қуриш (3-синф) ва криптотаҳлил масалаларини ечиш (4-синф) учун мўлжалланган хоссалар синфига бўлинган. Бунда, 3-синфга оид хоссалар 1-синфга тегишли хоссалар билан бир қаторда, 2-синф хоссаларининг биринчи қисмини, 4-синфга оид хоссалар эса 2-синфга тегишли хоссаларнинг қолган қисмини ўз ичига олади.

1-синфга оид хоссаларга қуйидагилар киради:

1.3.1-хосса. $a^{\backslash z+d} \equiv a^{\backslash z}$ ® $a^{\backslash d}$ $(mod\ n)$, $a^{\backslash z} \equiv a^{\backslash z}$®$0$ $(mod\ n)$, бу ерда ® — модуль n бўйича R параметрли кўпайтириш амалининг рамзи, 0 — бирлик элементи, $\backslash$ — параметр R билан даражага ошириш рамзи, $a, z, d \in \{1,2,..., n-1\}$;

1.3.2-хосса. $a^{\backslash z*d} \equiv (a^{\backslash z})^{\backslash d} \equiv (a^{\backslash d})^{\backslash z} (mod\ n)$, бу ерда $a \in \{1,2,..., n-1\}$, $\backslash$ — параметр R билан даражага ошириш рамзи, $z, d \in \{1,2, ..., \varphi(n) -1\}$;

Юқорида келтирилган хоссалар параметрли функция кийматини исталган даража кўрсаткичи учун эффектив ҳисоблаш учун етарлидир. Бу ерда катта даражага ошириш жараёни аввалги бандда кўрилганидек, экспоненциал функцияни ҳисоблаш жараёни каби кечиб, даврий тарзда $x=2$ (квадрат) даражага ошириш ва ҳосил бўлган аввалги натижани асосга параметрли кўпайтириш амалларидан фойдаланишдан иборат бўлади.

1.3.3-хосса. $a^{\backslash \varphi(n)+1} \equiv a (mod\ n)$, $a^{\backslash 1} = a$, бу ерда $\varphi(n)$ — Эйлер пи-функцияси, $a \in \{1,2,..., n-1\}$;

1.3.4-хосса. Агар d, e $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда $(a^{\backslash d})^{\backslash e} \equiv a (mod\ n)$, бу ерда $a \in \{1,2,..., n-1\}$, $\backslash$ — параметр R билан даражага ошириш рамзи; анъанавий даражага ошириш функциясида $(a^d)^e \equiv a\ (mod\ n)$.

Мисол:

n	$\varphi(n)$	e	d	R	a	$a^{\backslash d}$	$a=(a^{\backslash d})^{\backslash e}$
107	106	37	43	7	4	19	4
299	264	161	41	7	4	55	4

Юқорида келтирилган хоссалар учун $n \in \{p, p_1 * p_2\}$.

2-синфга оид хоссалардан криптография масалаларида (3-синф) (1-синфга оид хоссаларга қўшимча тарзда) қўллашга мўлжалланганларига қуйидагилар киради (айримлари келтирилган):

2.3.1-хосса. Параметри $R \geq 1$ бўлган ҳар қандай параметрли функция учун, агар R билан $p_1 * p_2$ ўзаро туб бўлиб, модуль $n=p$, $n=p_1 * p_2$ бўлса, унда Эйлер пи-функцияси $\varphi(n)$ қиймати мос тарзда $p-1$, $(p_1-1)*(p_2-1)$ ларга тенг, агар R билан p_1 ўзаро туб бўлиб, модуль $n=p_1 * p_2$ бўлса, унда Эйлер пи-функцияси $\varphi(n)$ қиймати $p_1*(p_2-1)$ га тенг, агар R билан p_2 ўзаро туб бўлиб, модуль $n=p_1 * p_2$ бўлса, унда Эйлер пи-функцияси $\varphi(n)$ қиймати $p_2*(p_1-1)$ га тенг.

Изоҳ: модуль $n = p_1 * p_2$ бўлганда, параметр R билан фақат p_1 ёки фақат p_2 ўзаро туб бўлса "Эйлер пи-функцияси $\varphi(n)$ қиймати" атамасидан фойдаланиш тўғри бўлмайди, чунки адабиётда Эйлер пи-функцияси $\varphi(n)$ қиймати деганда, n билан ўзаро туб сонлар назарда тутилади ва бу қиймат келтирилган ифода бўйича ҳисоблаш натижасидан кам чиқади. "Эйлер пи-функцияси $\varphi(n)$ қиймати" атамаси $\varphi(n)$ модуль бўйича ўзаро тескари даража кўрсаткичлари жуфтлигини ҳисоблашдаги вазифасига кўра ва қуйида келтирилган хоссалар мазмунига таъсир кўрсатмаслигини ҳисобга олиб, ундан вазифасига мос маънода фойдаланиш мақсадга мувофиқ бўлади. Аслида, бу атама "Вазифаси бўйича Эйлер пи-функцияси $\varphi(n)$ қиймати аналоги" маъносини ифода этади. Мазкур хосса параметрли функциянинг бошқа бир томонлама функциялардан тамойил жиҳатидан фарқини намоён этади.

2.3.2-хосса. $a^{\backslash 0} = 0$, $a^{\backslash -1} \equiv - a*(1+ R * a)^{-1} \pmod n$, бу ерда 0 — бирлик элементи, $a^{\backslash -1}$ — a нинг модуль n бўйича R параметрли тескари қиймати, $(1+ R*a)^{-1}$ -$(1+R * a)$ нинг модуль n бўйича тескари қиймати, $a \in \{1,2,.., n-1\}$.

2.3.3-хосса. $R*a^{\backslash x}\ (mod\ n) \equiv (1+R*a)^x - 1\ (mod\ n)$, бу ерда R — параметр, $a^{\backslash x}$ - a нинг параметр R билан x-даражаси қиймати, $(1+R*a)^x - (1+R*a)$ нинг x-даражаси қиймати $x \in \{1,2,\ldots, \varphi(n) - 1\}$, $a \in \{1,2,\ldots, n-1\}$.

Мисол:

n	R	a	x	$a^{\backslash x}$	$R*a^{\backslash x}$	$(1+R*a)^x-1$
107	13	6	19	23	85	85

Мазкур хосса асосида параметр R маълум бўлса, параметрли функция қийматидан анъанавий даражага ошириш функцияси қийматига ўтилади.

2.3.4-хосса. $a^{\backslash x+1} \equiv a * \Sigma^{i=x}_{i=0} F^i (mod\ n)$,

бу ерда R — параметр, $a^{\backslash x+1}$ — a нинг параметр R билан $(x+1)$ - даражаси қиймати, $F=1+R*a$, F^x — F нинг x-даражаси қиймати, $\Sigma^{i=x}_{i=0} F^i$ — F нинг 0 дан x гача даражаларининг йиғиндиси.

Мисол:

n	R	F	x	$a^{\backslash x+1}$	$a * \Sigma^{i=x}_{i=0} F^i$
107	19	21	2	65	65
391	19	25	2	349	349

2.3.5-хосса. Агар $R_1 \neq R_2 < n$, d_1, d_2 ва e_1, e_2 мос тарзда $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда

$(a^{\backslash d1})^{\backslash\backslash d2} \equiv s\ (mod\ n)$, $(s^{\backslash\backslash e2})^{\backslash e1} \equiv a\ (mod\ n)$,

бу ерда a, $s \in \{1,2,\ldots, n-1\}$, d_1, d_2, $e_1, e_2 \in \{1,2,\ldots, \varphi(n) - 1\}$, $^{\backslash}$ — параметр R_1 билан даражага ошириш рамзи, $^{\backslash\backslash}$ — параметр R_2 билан даражага ошириш рамзи.

Мисол:

n	p_1	p_2	$\varphi(n)$	R_1	R_2	a	d_1	d_2	e_2	e_1	s	$(s^{\backslash\backslash e2})^{\backslash e1}$
107	107		106	17	37	3	19	29	11	67	38	3
8881	107	83	8692	17	37	3	19	3297	29	915	679	3

2.3.6-хосса. Агар d, e $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда

$a * 1^{\backslash\backslash d} \equiv sa\ (mod\ n)$,

$sa * 1^{\backslash\backslash\backslash e} \equiv a\ (mod\ n)$,

бу ерда $a \in \{1,2,..., n-1\}$, sa — шифрматн, $^{\backslash\backslash}$ — параметр a билан даражага ошириш рамзи, $^{\backslash\backslash\backslash}$ — параметр sa билан даражага ошириш рамзи.

Мисол:

n	$\varphi(n)$	e	d	R	a	$I^{\backslash\backslash d}$	$sa = a*I^{\backslash\backslash d}$	$I^{\backslash\backslash\backslash e}$	$a = sa*I^{\backslash\backslash\backslash e}$
107	106	37	43	7	4	5	20	43	4
299	264	161	41	7	4	105	121	131	4

2.3.7-хосса. Агар d, e $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда

$a * I^{\backslash\backslash d} \equiv sa \ (mod\ n)$,

$sa * I^{\backslash\backslash\backslash e} \equiv a \ (mod\ n)$,

бу ерда $a \in \{1,2,..., n-1\}$, sa — шифрматн, $^{\backslash\backslash}$ — параметр a билан даражага ошириш рамзи, $^{\backslash\backslash\backslash}$ — параметр sa билан даражага ошириш рамзи.

Мисол:

n	$\varphi(n)$	e	d	R	a	$I^{\backslash\backslash d}$	$sa = a*I^{\backslash\backslash d}$	$I^{\backslash\backslash\backslash e}$	$a = sa*I^{\backslash\backslash\backslash e}$
107	106	37	43	7	4	5	20	43	4
299	264	161	41	7	4	105	121	131	4

2.3.8-хосса. $R_1^{-1} * a^{\backslash x} \ (mod\ n) \equiv (R_1^{-1} * a)^{\backslash\backslash x} \ (mod\ n)$,

$a * (R_1^{-1})^{\backslash\backslash\backslash x} \ (mod\ n) \equiv (R_1^{-1} * a)^{\backslash\backslash x} \ (mod\ n)$,

бу ерда R, R_1 — параметрлар, $a^{\backslash x}$ — a нинг параметр R билан x-даражаси қиймати, $(R_1^{-1} * a)^{\backslash\backslash x}$ — $(R_1^{-1} * a)$ нинг параметр $R*R_1 \equiv R*R_1 (mod\ n)$ билан x-даражаси қиймати, $(R_1^{-1})^{\backslash\backslash\backslash x}$ — R_1^{-1} нинг параметр $a*R*R_1 \equiv a*R*R_1 \ (mod\ n)$ билан x-даражаси қиймати, R_1^{-1} — R_1 нинг модуль n бўйича тескари қиймати, a, R, $R_1 \in \{1,2,..., n-1\}$, $x \in \{1,2,..., \varphi(n)-1\}$.

Мисол:

n	R	R_1	R_1^{-1}	a	x	$a^{\backslash x}$	$R_1^{-1} * a^{\backslash x}$	$(R_1^{-1}*a)^{\backslash\backslash x}$
107	13	8	67	6	19	23	43	43

n	R	R_1	R_1^{-1}	a	x	$(R_1^{-1})^{\backslash\backslash\backslash x}$	$a * (R_1^{-1})^{\backslash\backslash\backslash x}$	$(R_1^{-1} * a)^{\backslash\backslash x}$
107	13	8	67	6	19	25	43	43

Мазкур хосса асосида бошқа шаклдаги таққосламалар ҳам келиб чиқади. Масалан, *2.3.8-хосса*да $a^{\backslash x}$ ўрнига $(R_2^{-1}*a)^{\backslash x}$ ни қўйсак, *хосса* қуйидаги кўринишни олади:

$R_1^{-1}*(R_2^{-1}*a)^{\backslash x}(mod\ n) \equiv (R_1^{-1}*R_2^{-1}*a)^{\backslash\backslash x}\ (mod\ n)$, бу ерда R, R_1, R_2 — параметрлар, $(R_2^{-1} * a)^{\backslash x}$ — $(R_2^{-1} * a)$ нинг параметр $R*R_2 \equiv R*R_2 (mod\, n)$ билан x-даражаси қиймати, $(R_1^{-1}*R_2^{-1}*a)^{\backslash\backslash x}$ — $(R_1^{-1} * R_2^{-1} * a)$ нинг параметр $R*R_1*R_2 \equiv R*R_1*R_2 (mod\ n)$ билан x-даражаси қиймати, R^{-1}, R_1^{-1}, R_2^{-1} — мос тарзда R, R_1, R_2 нинг модуль n бўйича тескари қийматлари.

Мисол:

n	R	R^{-1}	R_2	R_2^{-1}	R_1	R_1^{-1}	a	x	$(R_2^{-1}*a)^{\backslash x}$	$R_1^{-1}*(R_2^{-1}*a)^{\backslash x}$	$(R_1^{-1}*R_2^{-1}*a)^{\backslash\backslash x}$
107	1	1	13	33	8	67	6	19	32	4	4

2.3.9-хосса. $R*1^{\backslash\backslash x}\ (mod\ n) \equiv R^{\backslash x}\ (mod\ n)$, бу ерда R — параметр, $1^{\backslash\backslash x}$ — 1нинг параметр R билан x-даражаси қиймати, $R^{\backslash x}$ — R нинг параметр $R=1$ билан x-даражаси қиймати, $x \in \{1,2,\ ..,\ \varphi(n-1)\}$.

Мисол:

n	R	x	$1^{\backslash\backslash x}$	$R*1^{\backslash\backslash x}$	$R^{\backslash x}$
107	13	19	43	24	24

2.3.10-хосса. $(R_1*a)^{\backslash x} \pm (R_2*a)^{\backslash\backslash x} \equiv (R*a)^{\backslash\backslash\backslash x}\ (mod\ n)$, бу ерда R_1, R_2, R — параметрлар, $R \equiv R_1 \pm R_2\ (mod\ n)$, $(R_1*a)^{\backslash x}$ — R_1*a нинг параметр R_1^{-1} билан x-даражаси қиймати, $(R_2*a)^{\backslash\backslash x}$ — R_2*a нинг параметр R_2^{-1} билан x-даражаси қиймати, $(R*a)^{\backslash\backslash\backslash x}$ — $R*a$ нинг параметр R^{-1} билан x-даражаси қиймати, R_1^{-1}, R_2^{-1}, R^{-1} — мос тарзда R_1, R_2 ва R нинг модуль n бўйича тескари қийматлари, $a \in \{1,2,\ ..,\ n-1\}$, $x \in \{1,2,\ ..,\ \varphi(n)-1\}$.

Мисол:

n	a	R_1	R_2	$R=R_1+R_2$	R_1^{-1}	R_2^{-1}	R^{-1}	x	$(R_1*a)^{\backslash x}$	$(R_2*a)^{\backslash\backslash x}$	$(R*a)^{\backslash\backslash\backslash x}$
107	29	13	5	18	33	43	6	17	51	69	13

n	a	R_1	R_2	$R=R_1-R_2$	R_1^{-1}	R_2^{-1}	R^{-1}	x	$(R1*a)^{\backslash x}$	$(R2*a)^{\backslash\backslash x}$	$(R*a)^{\backslash\backslash\backslash x}$
107	29	13	5	8	33	43	67	17	51	69	89

Мазкур китобда 2-синфга оид хоссалардан криптотаҳлил масалаларида (4-синф) қўллашга мўлжалланганларидан бирини келтириш билан чекланилган.

2.4.1-хосса (параметр R). Агар $n \in \{ p, p_1 * p_2 \}$ — модуль, $n > a \geq 1$, $R > e > 1$, $1 < R < \varphi(n)$, $y \equiv a^{\backslash e} \pmod n$, $y_1 \equiv a^{\backslash e-1} \pmod n$, $(a * y_1)$ билан n ўзаро туб бўлса, унда $R \equiv (y - y_1 - a) * (a * y_1)^{-1} \pmod n$.

Мисол:

n	a	x	y	y_1	R
23	19	6	27	5	4

Мазкур хосса асосида параметр R ни топишга уринган криптотаҳлилчи учун берилган модуль n, асос a билан бир қаторда, қўшни даража кўрсаткичлари жуфти $(x, x+1)$ учун даража қийматлари жуфти (y, y_1)нинг ҳам маълум бўлиши зарур ва етарли. Демак, махсус аппаратли криптографик модуль (7-бўлимга қаранг) ундан фойдаланувчилар криптографик модулга бир-биридан камида 2^{160} га фарқланмайдиган даража кўрсаткичларини киритишга йўл қўймайдиган ҳимоя механизмлари билан таъминланган бўлиши шарт.

Келтирилган параметрли функция хоссаларининг анъанавий экспоненциал функция хоссаларидан фарқли томонлари криптография ва криптотаҳлил масалаларига, шу жумладан, *дискрет логарифм ва факторлаштиришга* янгича ёндашувларни тақозо этади ҳамда криптологияда янги муаммоларни келтириб чиқаради. Бундай муаммолар қаторига мавжуд муаммолардан тамойилли фарқ этган *даража параметри муаммоси* [19-21,25, 26] ва унга мос бўлган *Диффи-Хэллман муаммоси* киради.

3.3 Матрицавий параметрли алгебрада даражага ошириш

Матрицавий параметрли алгебрадан фойдаланилганда криптоалгоритмлар криптобардошлилигини матрицавий параметр махфийлиги ҳисобига янада ошириш ва кичик модулга эга

бўлган калитлар орқали ҳам етарли криптобардошлиликка эга бўлган криптоалгоритмлар яратиш имконияти пайдо бўлади. Ушбу амаллар орқали ҳосил бўлган криптотизимлар нафақат юқори криптобардошлиликка эга бўлибгина қолмай, уларнинг тезлигини ҳам кескин ошириб юборади.

Берилган квадрат матрицани ўзига матрицавий параметрли кўпайтириш, яъни квадратлаш натижасида янги квадрат матрица ҳосил бўлади. Ҳосил бўлган квадрат матрицани дастлабки матрицага матрицавий параметрли кўпайтириш натижасида, дастлабки матрицанинг *3*-даражаси бўлган матрица ҳосил бўлади. Шу зайлда, матрицавий параметрли кўпайтириш натижасида, дастлабки матрицанинг исталган даражасини ҳосил қилиш мумкин.

3.1-жадвалда модуль $p=11$ бўйича 2х2 тартибли A

$$\begin{vmatrix} 9 & 4 \\ 3 & 1 \end{vmatrix}$$

учун матрицавий параметр $\underline{R}=E$

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$

бўлган дастлабки матрица A учун даража кўрсаткичлари ва даражалар қийматлари келтирилган.

3.1-жадвал

Даража кўрсаткичи	1	2	3	,	,	117	118	119	120	121
Даражалар қийматлари	9 4 3 1	1 4 3 4	9 5 1 10	, ,	, ,	10 1 9 8	2 2 7 9	2 5 1 3	0 0 0 0	9 4 3 1

3.1-жадвалда даража кўрсаткичи фақат $\varphi_m(p)=p^2-1=120=11^2-1$ га тенг бўлганда *0*-матрица ҳосил бўлади.

3.2-жадвалда модуль $p=11$ бўйича 3х3 тартибли матрица A

$$\begin{vmatrix} 4 & 6 & 8 \\ 3 & 1 & 2 \\ 7 & 9 & 5 \end{vmatrix}$$

учун матрицавий параметри $\underline{R}$

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$$

бўлган дастлабки матрица A учун даража кўрсаткичлари ва даражалар қийматлари парчаси келтирилган.

3.2-жадвал

Даража кўрсаткичи	*1*	*2*	*3*	.	.	*1318*	*1319*	*1320*	*1321*
Даража қийматлари	*4 6 8*	*5 4 7*	*7 4 3*	.	.	*2 8 9*	*4 2 6*	*0 0 0*	*4 6 8*
	3 1 2	*6 1 6*	*1 3 9*	.	.	*2 7 8*	*2 2 8*	*0 0 0*	*3 1 2*
	7 9 5	*0 4 2*	*1 2 1*	.	.	*0 1 10*	*9 6 3*	*0 0 0*	*7 9 5*

3.2-жадвалда даража кўрсаткичи фақат $1320=11^3-11$ га тенг бўлганда *0*-матрица ҳосил бўлади.

3.3-жадвалда модуль $p=7$ бўйича $4x4$ тартибли матрица A

$$\begin{vmatrix} 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 \\ 3 & 2 & 3 & 1 \\ 2 & 1 & 4 & 3 \end{vmatrix}$$

учун матрицавий параметри $\underline{R}=E$

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

бўлган дастлабки матрица A учун даража кўрсаткичлари ва даражалар қийматлари парчаси келтирилган.

3.3-жадвал

Даража кўрсаткичи	*1*	*2*	*3*	.	.	*2399*	*2400*	*2401*
Даража қийматлари	*3 4 5 6*	*2 0 6 1*	*3 4 1 0*	.	.	*3 1 3 0*	*0 0 0 0*	*3 4 5 6*
	4 5 3 1	*2 2 5 2*	*4 2 5 0*	.	.	*4 2 4 1*	*0 0 0 0*	*4 5 3 1*
	3 2 3 1	*6 5 5 0*	*6 3 5 5*	.	.	*6 5 5 4*	*0 0 0 0*	*3 2 3 1*
	2 1 4 3	*4 5 3 4*	*6 1 4 2*	.	.	*5 6 2 2*	*0 0 0 0*	*2 1 4 3*

3.3-жадвалда даража кўрсаткичи фақат $2400=7^4-1$ га тенг бўлганда 0-матрица ҳосил бўлади.

Бу ерда ҳам, аввал кўриб ўтилганидек, матрицанинг e-даражасини ҳисоблашда e ни 2 нинг даража қийматларини ўз ичига олган ва унга тенг бўлган кўринишга келтириб, рекурсив тарзда ҳисобланади.

Масалан, A нинг $e=37$ матрицавий параметр $\underline{R}$ учун даражаси қуйидагича ҳисобланади:

$$A^{\backslash 37}=A^{\backslash 32+4+1}\equiv(((((A^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2}\underline{\circledR}\,(A^{\backslash 2})^{\backslash 2})\,\underline{\circledR}\,A\ (mod\ p),$$

бу ерда $A^{\backslash 2}\equiv 2xA+Ax\,\underline{R}xA\ (mod\ p)$.

Шуни таъкидлаш лозимки, матрицани матрицавий параметрли даражага ошириш функцияси бир томонлама функция бўлиб, у носимметрик криптотизимлар яратиш учун аҳамиятга моликдир.

Матрица A нинг e-даражаси $A^{\backslash e}$ билан белгиланади. Бу ерда $^{\backslash e}$ — матрицавий параметр билан e — даражага ошириш амалининг рамзидир.

Матрицавий параметрли тескарилаш амали қуйидаги ифода бўйича ҳисобланади:

$$A^{\backslash -1}\equiv -Ax(E+Ax\underline{R})^{-1}(mod\ p).$$

Бу ерда $^{-1}$ — матрицавий тескарилаш, E — бирлик матрицаси рамзларидир. Матрицавий параметрли тескари матрица $A^{\backslash -1}$ ни ҳисоблаш A матрица элементларининг қарама-қарши қийматларидан тузилган матрица — A ни шакллантириш, $(E+Ax\underline{R})$ $(mod\ p)$ ни ҳисоблаш, $(E+Ax\underline{R})$ га тескари матрица $(E+AxR)^{-1}$ ни ҳисоблаш ва уни чапдан — A га матрицавий кўпайтириш амалларини ўз ичига олади.

Берилган A матрицага матрицавий параметрли тескари матрица $A^{\backslash -1}$

$$A\,\underline{\circledR}A^{\backslash -1}\equiv 0\ (mod\ n)$$

аксиомани қаноатлантиради. Бу ерда 0 — 0 элементлардан шаклланган матрицавий параметрли бирлик матрицаси бўлиб,

$$A\,\underline{\circledR}0\equiv A\ (mod\ n)$$

аксиомани қаноатлантиради.

Қуйида модуль $p=257$ ва $\underline{R}=E$ бўлганда, $4x4$-тартибли матрица A га матрицавий параметрли тескари матрица $A^{\backslash -1}$ ни ҳосил

қилиш жараёни ва A , $A^{\backslash -1}$ матрицалари учун $A \circledR A^{\backslash -1} \equiv 0 (mod\ n)$ аксиома қаноатлантирилиши акс этган.

$$-A \times (E + A \times \underline{R})^{-1} \equiv A^{\backslash -1}$$

$$\begin{vmatrix} 243 & 1 & 2 & 3 \\ 3 & 241 & 3 & 3 \\ 2 & 4 & 240 & 2 \\ 3 & 5 & 6 & 243 \end{vmatrix} \times \left(\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} + \begin{vmatrix} 14 & 256 & 255 & 254 \\ 254 & 16 & 254 & 254 \\ 255 & 253 & 17 & 255 \\ 254 & 252 & 251 & 14 \end{vmatrix} \times \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} \right)^{-1} \equiv \begin{vmatrix} 191 & 210 & 87 & 92 \\ 112 & 201 & 112 & 112 \\ 103 & 112 & 192 & 103 \\ 254 & 137 & 12 & 96 \end{vmatrix}$$

$$A \circledR A^{\backslash -1} \equiv 0$$

$$\begin{vmatrix} 14 & 256 & 255 & 254 \\ 254 & 16 & 254 & 254 \\ 255 & 253 & 17 & 255 \\ 254 & 252 & 251 & 14 \end{vmatrix} \circledR \begin{vmatrix} 191 & 210 & 87 & 92 \\ 112 & 201 & 112 & 112 \\ 103 & 112 & 192 & 103 \\ 254 & 137 & 12 & 96 \end{vmatrix} \equiv \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix}$$

Таъриф. Матрицавий параметрли алгебрада даражага ошириш функциясини матрицавий параметрли функция деб номлаймиз.

Матрицавий параметрли алгебралардан фойдаланиш мавжуд криптотизимларни такомиллаштириш, уларнинг криптобардошлилигини ошириш, янги криптоалгоритм ва протоколлар яратиш нуқтаи назаридан аҳамиятга моликдир.

3.4 Бир томонлама матрицавий параметрли функциянинг хоссалари

Маълумки криптография соҳасида юқори криптобардошлиликка эга бўлган алгоритмлар ишлаб чиқиш муҳим вазифалардан ҳисобланади. Бир томонлама матрицавий параметрли функция криптография масалаларини ҳал қилишда ишлатилса, кичик модуль қўлланилганда ҳам юқори криптобардошлиликка эга бўлган криптотизимлар ишлаб чиқиш имконияти туғилади.

Матрицавий параметрли функция деганда, модуль арифметикасида матрицавий параметр $\underline{R}$ билан кўпайтириш амали

асосида бутун сонли даражага ошириш функцияси тушунилади. Қуйида асосан туб сонли модуль p бўйича аниқланган матрицавий параметрли функциянинг хоссалари баён қилинган. Чунки, иккита ҳар хил туб сонларнинг кўпайтмасидан иборат мураккаб модулдан фойдаланилганда матрицавий параметрли функция асосида қуриладиган криптотизимларнинг криптобардошлилиги факторлаш муаммоси билан чегараланиб, туб модулдан фойдаланган ҳолдаги каби криптобардошлиликнинг ортишига олиб келмайди. Қуйидаги келтирилган хоссаларда модуль p бўйича mхm тартибли матрица A ни mхm тартибли матрицавий параметр $\underline{R}$ билан e- даражаси $A^{\backslash e}(mod\ p)$ шаклида ифодаланган, бу ерда $e \in \{0, 1, -1, e, d, z\}$, $m<<p$, $^{\backslash}$ — матрицавий параметр $\underline{R}$ билан даражага ошириш рамзидир.

1-хосса. Ҳар қандай mхm тартибли матрица A ва матрицавий параметр $\underline{R}$ берилган бўлса, матрицавий параметрли функция учун, агар модуль p туб сон бўлса, унда Эйлер пи-функцияси $\varphi_m(p)$ қиймати p^m-1 ёки p^m-p га тенг.

2-хосса. $A^{\backslash 0} = 0$, $A^{\backslash 1} = A$, $A^{\backslash -1} \equiv -A\text{x}(E+A\text{x}\underline{R})^{-1}\ (mod\ p)$, бу ерда ноль-матрица 0 — бирлик элементи, $A^{\backslash -1}$ — A нинг модуль p бўйича матрицавий параметр $\underline{R}$ билан тескари матрицаси, $(E+A\text{x}\underline{R})^{-1}$ — номахсус матрица $(E+A\text{x}\underline{R})$ нинг модуль p бўйича тескари матрицаси.

3-хосса. $A^{\backslash z+d} \equiv A^{\backslash z}\ \underline{®}\ A^{\backslash d}\ (mod\ p)$, $A^{\backslash z} \equiv A^{\backslash z}\underline{®}0\ (mod\ p)$, бу ерда $\underline{®}$ — модуль p бўйича матрицавий параметр $\underline{R}$ билан кўпайтириш амали рамзи, ноль-матрица 0 — бирлик элементи, $z, d \in \{1,2,\ldots, \varphi_m(p)-1\}$.

4-хосса. $A^{\backslash z*d} \equiv (A^{\backslash z})^{\backslash d} \equiv (A^{\backslash d})^{\backslash z}\ (mod\ p)$, бу ерда $z, d \in \{1,2,\ldots, \varphi_m(p)-1\}$.

Юқорида келтирилган хоссалар матрицавий параметрли функция қийматини исталган даража кўрсаткичини эффектив ҳисоблаш учун етарлидир. Бу ерда, экспоненциал функцияни катта даражага ошириш жараёни каби даврий тарзда $x=2$ (квадрат) даражага ошириш ва ҳосил бўлган аввалги натижани асосга матрицавий параметр билан кўпайтириш амалларидан фойдаланилади.

Матрицавий параметрли функцияга қуйидаги хоссалар ҳам оиддир:

5-хосса. $A^{\varphi m(p)+1} \equiv A \ (mod\ p)$, бу ерда $\varphi_m(p)$ — Эйлер пи-функцияси.

6-хосса. Агар d, e $\varphi_m(p)$ билан ўзаро туб бўлиб, $\varphi_m(p)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда

$(A^d)^e \equiv A \ (\mathrm{mod}\ p)$.

7-хосса. $\underline{R}_1^{-1} \times A^e \ (mod\ p) \equiv (\underline{R}_1^{-1} \times A)^{\backslash e} \ (mod\ p)$, бу ерда $\underline{R}$, $\underline{R}_1$ — матрицавий параметрлар, A^e - A нинг матрицавий параметр $\underline{R}$ билан e-даражаси қиймати, $(\underline{R}_1^{-1} \times A)^{\backslash e}$ - $(\underline{R}_1^{-1} \times A)$ нинг матрицавий параметр $\underline{R} \times \underline{R}_1 \equiv \underline{R} \times \underline{R}_1 \ (mod\ p)$ билан e-даражаси қиймати, $\underline{R}^{-1}$, $\underline{R}_1^{-1}$ — мос тарзда $\underline{R}$ ва $\underline{R}_1$ нинг модуль p бўйича тескари қийматлари, $e \in \{1,2,\ldots, \varphi_m(p)-1\}$.

Мисол: Бу ерда модуль $p=257$.

$\underline{R}=\underline{R}_1$				A^5				$\underline{R}_1^{-1}$			
15	256	255	254	191	56	178	43	192	210	87	92
254	17	254	254	119	29	196	106	112	202	112	112
255	253	18	255	47	2	214	169	103	112	193	103
254	252	251	15	232	232	232	232	254	137	12	97

$\underline{R}_1^{-1} \times A$				$\underline{R} \times \underline{R}_1$				$\underline{R}_1^{-1} \times A^5 = (\underline{R}_1^{-1} \times A)^5$			
137	204	14	81	241	248	212	174	229	67	162	0
245	12	36	60	176	62	176	176	92	45	255	208
141	138	135	132	209	129	95	209	176	145	114	83
252	238	224	210	194	124	80	4	248	119	247	118

Мазкур хосса асосида бошқа шаклдаги таққосламалар ҳам келиб чиқади. Масалан, *7-хосса*да A^e ни ўрнига $(\underline{R}_2^{-1} \times A)^e$ қўйсак, *7-хосса* қуйидаги кўринишга эга бўлади:

8-хосса. $\underline{R}_1^{-1} \times (\underline{R}_2^{-1} \times A)^e (mod\ p) \equiv (\underline{R}_1^{-1} \times \underline{R}_2^{-1} \times A)^{\backslash e} \ (mod\ p)$, бу ерда $\underline{R}$, $\underline{R}_1$, $\underline{R}_2$ — матрицавий параметрлар, $(\underline{R}_2^{-1} \times A)^e$ — $(\underline{R}_2^{-1} \times A)$ нинг матрицавий параметр $\underline{R} \times \underline{R}_2 \equiv \underline{R} \times \underline{R}_2 \ (mod\ p)$ билан e-даражаси қиймати, $(\underline{R}_1^{-1} \times \underline{R}_2^{-1} \times A)^{\backslash e}$ — $(\underline{R}_1^{-1} \times \underline{R}_2^{-1} \times A)$ нинг матрицавий параметр $\underline{R} \times \underline{R}_1 \times R_2 \equiv \underline{R} \times \underline{R}_1 \times \underline{R}_2 \ (mod\ p)$ билан e-даражаси қиймати, $\underline{R}^{-1}$,

$\underline{R}_1^{-1}$, $\underline{R}_2^{-1}$ — мос тарзда $\underline{R}$, $\underline{R}_1$, $\underline{R}_2$ нинг модуль p бўйича тескари матрицалари.

9-хосса. $\underline{R}$x$A^{\backslash e}$ $(mod\ p) \equiv (E+\underline{R}\ \text{x}\ A)^e - E$ $(mod\ p)$, бу ерда $\underline{R}$ — матрицавий параметр, $A^{\backslash e}$ — A нинг матрицавий параметр $\underline{R}$ билан e-даражаси қиймати, $(E+\underline{R}\text{x}A)^e$ — $(E+\underline{R}\text{x}A)$ нинг e-даражаси қиймати, $e \in \{1,2,..,\varphi_m(p)-1\}$.

Мисол: Бу ерда модуль $p=31$, $e=17$.

A				$\underline{R}$				$A^{\backslash 17}$			
1	5	8	9	1	2	3	4	13	10	21	3
11	15	13	14	5	6	7	8	12	2	8	20
21	22	23	24	9	10	11	12	30	30	24	8
29	28	27	26	13	14	15	16	21	10	10	5

$\underline{R}$x$A^{\backslash 17}$				$E+\underline{R}$xA				$(E+\underline{R}$x$A)^{17}-E$			
25	20	25	25	17	27	25	27	25	20	25	25
19	11	29	14	16	29	30	9	19	11	29	14
13	2	2	3	16	29	5	22	13	2	2	3
7	24	6	23	16	30	9	5	7	24	6	23

10-хосса. $\underline{R}$x$E^{\backslash e}$ $(mod\ p) \equiv \underline{R}^{\backslash\backslash e}$ $(mod\ p)$, бу ерда $\underline{R}$ — матрицавий параметр, $E^{\backslash e}$ — E нинг матрицавий параметр $\underline{R}$ билан e-даражаси қиймати, $\underline{R}^{\backslash\backslash e}$ — $\underline{R}$ нинг матрицавий параметр $\underline{R}= E$ билан e-даражаси қиймати, $e \in \{1,2,..,\varphi_m(p)-1\}$.

Мисол: Бу ерда модуль $p=31$, $e=17$.

$\underline{R}$				$E^{\backslash 17}$				$\underline{R}$x$E^{\backslash 17}=\underline{R}^{\backslash\backslash 17}$			
1	2	3	4	29	20	28	5	12	1	21	10
5	6	7	8	29	30	28	12	29	4	10	16
9	10	11	12	15	6	14	19	15	7	30	22
13	14	15	16	1	30	28	12	1	10	19	28

11-хосса. $A^{\backslash e+1} \equiv (\Sigma^{i=e}_{i=0} F^i)xA$ $(mod\ p)$, бу ерда $\underline{R}$ — матрицавий параметр, $A^{\backslash e+1}$ — A нинг матрицавий параметр R билан $(e+1)$-даражаси қиймати, $F=E+A\text{x}\underline{R}$, F^e — F нинг e-даражаси қиймати, $\Sigma^{i=e}_{i=0} F^i$ — F нинг 0 дан e гача даражаларининг йиғиндиси.

Мисол: Бу ерда модуль $p=31$, $e=5$.

A				$\underline{R}$				$A^{\backslash 6}$			
1	5	8	9	1	2	3	4	11	12	5	21
11	15	13	14	5	6	7	8	25	3	14	8
21	22	23	24	9	10	11	12	27	12	21	23
29	28	27	26	13	14	15	16	17	7	14	10

R				$E+A*\underline{R}$				$\Sigma^{i=e}_{i=0} F^i$				$(\Sigma^{i=e}_{i=0} F^i)xA$			
1	2	11	15	25	4	11	12	5	21	3	4	30	21	13	5
5	6	25	11	16	27	25	3	14	8	7	8	13	5	26	17
9	10	29	17	11	24	27	12	21	23	11	12	30	27	25	21
13	14	1	28	24	26	17	7	14	10	15	16	6	23	9	27

12-хосса. Агар $\underline{R}_1 \neq \underline{R}_2$, d_1, d_2 ва e_1, e_2 мос тарзда $\varphi_m(p)$ билан ўзаро туб бўлиб, $\varphi_m(p)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда

$(A^{\backslash d1})^{\backslash\backslash d2} \equiv S \pmod p$, $(S^{\backslash\backslash e2})^{\backslash e1} \equiv A \pmod p$,

бу ерда A, S — квадрат матрицалар, d_1, d_2, $e_1, e_2 \in \{1,2,..,\varphi_m(p)-1\}$, $^{\backslash}$ — матрицавий параметр $\underline{R}_1$ билан даражага ошириш рамзи, $^{\backslash\backslash}$ — матрицавий параметр $\underline{R}_2$ билан даражага ошириш рамзи.

Мисол: Бу ерда модуль $p=7$, $\varphi_m(p)_{R1}=342$, $k=7$, $\varphi_m(p)_{R2}=2400$, $d_1=29$, $d_2=1553$, $e_2=17$, $e_1=59$.

A				$\underline{R}_1$				$\underline{R}_2$			
1	5	1	2	1	1	3	4	2	5	3	6
4	1	6	0	5	6	0	1	1	6	5	1
3	6	2	3	2	3	4	5	3	1	6	2
1	0	6	5	6	5	1	6	5	2	3	2

$A^{\backslash 29}$				$S=(A^{\backslash 29})^{\backslash\backslash 1553}$			
2	1	0	6	6	2	5	2
2	5	2	4	1	3	4	1
0	2	1	1	3	1	2	3
2	1	4	4	2	1	2	0

$S^{\backslash\backslash 17}$				$(S^{\backslash\backslash 17})^{\backslash 59}$			
2	1	0	6	1	5	1	2
2	5	2	4	4	1	6	0
0	2	1	1	3	6	2	3
2	1	4	4	1	0	6	5

Юқорида келтирилган матрицавий параметрли функция хоссаларининг матрицавий экспоненциал функция хосса-

ларига ўхшаш томонлари ҳам, ундан фарқли томонлари ҳам мавжуд.

Ўхшаш томонларга қуйидагилар киради:

a) асоснинг биринчи даражаси ўзига тенглиги бир хил;

b) юқори даражага ошириш жараёни бир хил кечади ва амаллар сони тахминан иккита матрицавий кўпайтириш амалига ортиқ;

c) *3-6*-хоссалар даражага ошириш рамзи аниқлигида айнандир.

Фарқли томонларга қуйидагилар киради:

a) бирлик элементи *0*- матрицага тенг;

b) *1,2, 7-12*-хоссалар фарқли.

Келтирилган матрицавий параметрли функция хоссаларининг яратилиши мумкин бўлган матрицавий экспоненциал функция хоссалардан фарқли томонлари криптотизимлар яратишга ва криптотаҳлил масалаларига янгича ёндашувларни тақозо этади. Янги муаммолар қаторига матрицавий даража параметри ва унга мос Диффи-Хэллман муаммоси киради.

3-бўлим бўйича хулосалар

1. Модуль арифметикасида анъанавий бир томонлама дискрет даражага ошириш функцияси параметр *R=1* бўлган диаматрица-устунлар алгебраси ва параметрли алгебрада параметрли дискрет даражага ошириш (диаалмаштиришлар) функциясининг хусусий ҳолидир. Параметр *R* диаматрица-устунлар алгебрасида берилган бир элементли диаматрица-устун элементига тенг бўлса, параметрли алгебрада *R* ихтиёрий натурал сондир. Бир томонлама бутун сонли ва матрицавий параметрли функцияни ҳисоблаш жараёни анъанавий бир томонлама дискрет даражага ошириш функциясини ҳисоблаш жараёни каби осон амалга оширилади.

2. 2 хил модуль $n \in \{p,\ p_1{*}p_2\}$ бўйича аниқланган параметрли функциянинг хоссалари 2 та белги асосида 2 синфга бўлинган: булар анъанавий даражага ошириш функциясига ўхшаш (1-синф) ва фарқли (2-синф) хоссалар бўлиб, ўз навбатида мазкур синфларга оид хоссалар муаллиф томонидан

фойдаланишга мўлжалланганлигига қараб, криптографик тизимлар қуриш (3-синф) ва криптотаҳлил масалаларини ечиш (4-синф) учун мўлжалланган хоссалар синфларига бўлинади. Бунда, 3-синфга оид хоссалар 1-синфга тегишли хоссалар билан бир қаторда, 2-синф хоссаларининг биринчи қисмини, 4-синфга оид хоссалар эса 2-синфга тегишли хоссаларнинг қолган қисмини ўз ичига олади.

3. Параметрли функция хоссаларининг анъанавий экспоненциал функция хоссаларидан фарқли томонлари, криптотаҳлил йўналишида ва криптографияда янги муаммоларни таърифлаб беради. Модуль $n=p_1*p_2$ бўлганда, параметр R билан p_1 ёки p_2 ўзаро туб бўлса "Эйлер пи-функцияси $\varphi(n)$ киймати" атамасидан фойдаланиш тўғри бўлмайди, чунки Эйлер пи-функцияси $\varphi(n)$ қиймати деганда, n билан ўзаро туб сонлар сони назарда тутилади ва бу қиймат келтирилган ифода бўйича ҳисоблаш натижасидан кам чиқади. "Эйлер пи-функцияси $\varphi(n)$ қиймати" атамаси $\varphi(n)$ модуль бўйича ўзаро тескари даража кўрсаткичлари жуфтлигини ҳисоблашдаги вазифасига мос маънода фойдаланиш мақсадга мувофиқ бўлади. Аслида, бу атама "Вазифаси бўйича Эйлер пи-функцияси $\varphi(n)$ қиймати аналоги" маъносини ифода этади. Мазкур ҳолат параметрли функциянинг бошқа бир томонлама функциялардан тамойилли фарқини намоён этади.

4. Матрицавий параметрли функциянинг хоссалари мажмуида матрицавий экспоненциал функция хоссаларига ўхшаш томонлари ҳам, ундан фаркли томонлари ҳам мавжуд. Ўхшаш томонлари, бир томонлама матрицавий параметрли функция асосида, барча бир томонлама матрицавий дискрет даражага ошириш функцияси асосида ишлаб чиқилиши мумкин бўлган криптотизимларни такомиллаштириш имконини беради. Фарқли томонлари, матрицавий параметрли функция асосида мавжуд криптотизимлардан тамойилли фарқли криптотизимлар яратиш учун замин яратади.

4-БЎЛИМ

ПАРАМЕТРЛИ ФУНКЦИЯ ХОССАЛАРИГА ОИД МУАММОЛАР

Тўрт синфга бўлинган 3-бўлимда келтирилган параметрли функция хоссаларидан учинчи синфи асосан параметр R нинг махфийлиги ҳисобига криптографик тизим криптобардошлилигини оширишга хизмат қилади. Қуйида шу параметрни топишга йўналтирилган даража параметри муаммоси, унга мос Диффи-Хэллман муаммоси баён қилинган.

4.1 Даража параметри муаммоси

Мазкур китобда ишлаб чиқилган носимметрик криптографик тизимларда модуль сифатида туб ёки таркибли сондан фойдаланилган бўлиб, тизим криптобардошлилигининг ортиши бир томонлама параметрли функция ифодасида қатнашадиган даражага ошириш параметри (қисқача, даража параметри) R ноқонуний фойдаланувчилардан сир сақланишига асосланади. Криптографияга оид нашрларда бунга ўхшаш муаммо келтирилмаган.

Даража параметри муаммоси учта мураккаблик поғонаси билан фарқланиб, қуйидагича таърифланади [21, 25]:

1-таъриф. Агар параметрли алгебра $(F_n; \circledR)$ да ташувчи F_n нинг элементи y берилган бўлса, унда параметр R, даража кўрсаткичи e ва элемент a топилсин, бу ерда F_n — n та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ — a ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash\omega}$ $(mod\ n) \equiv 0$ шартини фақат $\omega=q$ бўлгандагина қаноатлантиради, q — $\varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ — *Эйлер пи-функцияси* (мураккабликнинг учинчи поғонасига оид муаммо).

2-таъриф. Агар параметрли алгебра $(F_n; \circledR)$ да ташувчи F_n нинг элементлари y ва a берилган бўлса, унда параметр R ва даража кўрсаткичи e топилсин, бу ерда F_n — n та бутун сонлар-

дан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ — a ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash \omega}$ $(mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, q — $\varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ — *Эйлер пи-функцияси* (мураккабликнинг иккинчи поғонасига оид муаммо).

3-таъриф. Агар параметрли алгебра $(F_n;$ ®) да ташувчи F_n нинг элементлари y, a ва даража кўрсаткичи e берилган бўлса, унда параметр R топилсин, бу ерда F_n — n та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ — a ни параметр R билан e—даражаси рамзи, элемент a $a^{\backslash \omega}$ $(mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, q — $\varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ — *Эйлер пи-функцияси* (мураккабликнинг биринчи поғонасига оид муаммо).

Мазкур муаммоларнинг юзага чиқиши бир томонлама параметрли функциянинг қуйидаги 2.3.4-хоссаси билан боғлиқ:

$$a^{\backslash e} \equiv a^* \Sigma_{i=0}^{i=e-1} F^i (mod\ n), \qquad (4.1)$$

бу ерда $F=1+R^*a$, $n \in \{p, p_1^* p_2\}$.

Муаллифга бу муаммони эффектив ечиш усули маълум эмас.

Даража параметри муаммосига берилган 1-, 2- ва 3-таърифларда номаълумлар сонини эътиборга олсак, муаммони ҳал этиш мураккаблиги ўзаро мос тарзда учинчи, иккинчи ва биринчи поғонага оид деб ҳисоблаш ўринлидир.

Параметр ***R*** берилганда қонуний фойдаланувчилар учун даража параметри муаммоси қуйидагича таърифланади:

4-таъриф. Агар параметрли алгебра $(F_p;$ ®) да ташувчи F_p нинг элементлари y ва R берилган бўлса, унда даража кўрсаткичи e ва элемент a топилсин, бу ерда F_p — n та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ p)$, $^{\backslash e}$ — a ни параметр R билан e-даражаси рамзи, элемент a $a^{\backslash \omega}$ $(mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, q - $\varphi()$ нинг бутун сонли бўлувчиси, $\varphi(n)$ — *Эйлер пи-функцияси.*

4-таърифга тааллуқли даража параметри муаммосини $n=p$ бўлганда унинг дискрет логарифм муаммосига осонгина

келтиришини эътиборга олиб, дискрет диалогарифм муаммоси деб аташ мумкин ва уни ечиш мураккаблиги, параметр берилгани сабабли, нолинчи даражага тегишли десак хато бўлмайди.

Муаммолар учун юқорида келтирилган таърифлар *ташқи ва ички бадният бузгунчилар учун криптоалгоритмларнинг ҳар хил бардошлиликка эга бўлишини кўрсатади.*

4-таърифда акс этган муаммо ЭРИ бўйича O'z DSt 1092:2005 татбиқан куйидаги иккита дискрет логарифмлаш масаласини ечишга келтирилади:

$$y \equiv z^{\backslash i} \ (mod\ p) \tag{4.2}$$

бу ерда $i \equiv x^{*}u^{-1}(mod\ q)$,

$$y \equiv (m^{\backslash -1}\text{®}\ r)^{\backslash j}(mod\ p) \tag{4.3}$$

бу ерда $j \equiv x^{*}(-k)^{-1}(mod\ q)$.

Бузғунчининг ҳисоблаш ресурслари етарли бўлганда ЭРИ-нинг ёпиқ калити (x, u, a) аниқ топилади. Шундай қилиб, O'z DSt 1092:2005 нинг криптобардошлилиги бир хил туб модуль p учун *АҚШ давлат стандарти DSA* га нисбатан икки марта юқори, сеанс калитли маромда эса беҳад юқори бўлади [25].

Даража параметри муаммосига берилган 1-, 2- ва 3-таърифларда *иккита ҳар хил даража параметри ишлатилишига оид 2.3.5-хосса эътиборга олинса* даража параметри муаммосини ҳал этиш мураккаблиги поғонаси янада юксалади. Қуйида 3-таърифга тегишли таърифни келтириш билан чекланамиз:

3'-таъриф. Агар параметрли алгебра (F_n; ®) да ташувчи F_n нинг элементлари y, a ва даража кўрсаткичлари e_1, e_2 берилган бўлса, унда параметр R_1 ва R_2 топилсин, бу ерда F_n — n та бутун сонлардан тузилган чекли тўплам, $y \equiv (a^{\backslash e1})^{\backslash e2}(mod\ n)$, $^{\backslash e1}$ — a ни параметр R_1 билан e_1-даражаси рамзи, $^{\backslash e2}$ — a ни параметр R_2 билан e_2-даражаси рамзи, $R_1 \neq R_2 < n$, элемент a $a^{\backslash \omega}$ $(mod\ n) \equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, q — $\varphi(n)$ нинг бутун сонли бўлувчиси, $\varphi(n)$ — *Эйлер пи-функцияси.*

Муаллиф томонидан олиб борилган дастлабки тадқиқотлар *3'-таърифда берилган муаммони ечиш мураккаблиги тенг*

модулда дискрет логарифм муаммосини ечиш мураккаблигидан кам бўлмаслигини кўрсатди, шу сабабли, 4-таърифга оид муаммони ечиш мураккаблигини нолинчи даражада деб ҳисобланди.

Даража параметри муаммосининг юзага келиши тамойилли янгича ёндашувга асосланган криптотизимлар яратишга имконият туғдиради.

Криптобардошлилиги даража параметри муаммосини ҳал этишнинг биринчи мураккаблик поғонасига асосланган криптография тизимларида модуль $n \geq 2^{256}$, даража кўрсаткичи туб сон бўлиб, $e \geq 2^{160}$ шартларига жавоб бериши лозимлиги тавсия этилади. Шу билан бир қаторда, махфий параметр $2^{256} > R$, $R^{-1} \geq 2^{160}$ шартини қондириши зарур. Кейинги бандларда келтирилган муаммоларнинг мураккаблиги ҳам биринчи галда даража параметри муаммоси билан боғлиқ.

4.2 Даража параметри муаммосига мос Диффи-Хэллман муаммоси

6-бўлимда келтирилган криптографик тизимларнинг бир қанчасида модуль сифатида туб сондан фойдаланилган бўлиб, уларнинг криптобардошлилиги даража параметри муаммосининг мураккаблигига асосланган. Шунингдек, уларнинг баъзиларида махфий асос ва\ёки махфий параметр ишлатилган. Даража параметри муаммоси параметрнинг махфийлигини, асоснинг эса махфий ёки ошкора бўлишини назарда тутади. Унинг таърифида чекли майдон учун параметрли ҳосил қилувчи (генератор, бошланғич илдиз) элементи тушунчасидан фойдаланилган.

Таъриф. Чекли майдон $GF(p)$ нинг параметр R билан ҳосил қилувчи (генератор, бошланғич илдиз) элементи шундай элемент a ки, унинг учун аниқланган барча даража кўрсаткичларининг ягона қиймати $p-1$ дагина параметрли функциянинг қиймати 0 га тенгдир.

$GF(p)$ чекли майдоннинг ҳосил қилувчи элементи a номаълум бўлганда даража параметри муаммоси янада мураккаблашади.

Кўриб ўтилган муаммоларнинг юзага келиши криптография коммуникация тизимларини янгича ёндашувлар асосида яратиш имкониятини туғдиради. 3-, 2-, 1-мураккаблик поғонасига эга ҳар бир даража параметри муаммосини ечиш учун аввало параметр R ни топиш керак. Ундан сўнг бу муаммони дискрет логарифм муаммосига келтириш мумкин. Аммо, параметр R ни кетма-кет танлаш усули, яъни кучли ҳужум усулидан ўзгача топиш усули ҳозиргача маълум эмас. Шунинг учун ҳам бу муаммо етарлича мураккабдир.

Агар параметр R маълум бўлса, даража параметри муаммоси дискрет логарифм муаммосига 2.3.*8*, 2.3.*3*-хоссалар асосида қуйидагича келтирилади:

Берилган: $y \equiv (a*R^{-1})^{\backslash x} (mod\ p)$

$\Downarrow$

$R_1^{-1} * a^{\backslash x} (mod\ p) \equiv (R_1^{-1} * a)^{\backslash\backslash x} (mod\ p)$ (2.3.8-хосса, $R=1$ учун)

$\Downarrow R_1$ ўрнига R қўйиш

$(a * R^{-1})^{\backslash x} (mod\ p) \equiv R^{-1} * a^{\backslash\backslash x} (mod\ p)$

$\Downarrow$ таққосламани R га кўпайтириш

$R * (a*R^{-1})^{\backslash x} (mod\ p) \equiv a^{\backslash\backslash x} (mod\ p)$

$\Downarrow$ (*2.3.3*-хосса, $R=1$ учун)

$a^{\backslash\backslash x} (mod\ p) \equiv (1+a)^x - 1\ (mod\ p)$

$\Downarrow$ таққосламага 1 ни қўшиш

$1 + a^{\backslash\backslash x} (mod\ p) \equiv (1+a)^x (mod\ p)$

$\Downarrow$ дискрет логарифм муаммоси

$1 + R * y\ (mod\ p) \equiv (1+a)^x (mod\ p)$.

Дискрет логарифм муаммоси: туб p, Z_p^* ҳосил қилувчи $1+a$ ва $1+R*y \in Z_p^*$ элемент берилган, шундай $0 \le x \le p-2$ бўлган бутун x сонни топингки, унда $(1+a)^x \equiv 1+R*y\ (mod\ p)$ бўлсин.

Дискрет логарифм муаммоси Диффи-Хэллман муаммосига асос бўлгани каби, даража параметри муаммоси асосида унга мос Диффи-Хэллман муаммоси келиб чиқади.

Даража параметри муаммосига мос Диффи-Хэллман муаммоси қуйидагича таърифланади:

агар туб модуль p, $GF(p)$ чекли майдоннинг ҳосил қилувчи (генератор) элементи $(a+1)$ ва параметрлар R_1, R_2 билан мос тарзда даражага ошириш функциялари қийматлари $Y_1 \equiv (a*R_1^{-1})\backslash e \pmod p$, $Y_2 \equiv (a*R_2^{-1})\backslash d \pmod p$ берилган бўлса, R_1, R_2 ва $((a*R_1^{-1})\backslash e * *R_2^{-1})\backslash\backslash d \pmod p \equiv ((a*R_2^{-1})\backslash d * R_1^{-1})\backslash\backslash e \pmod p$ топилсин, бу ерда R_1^{-1} — R_1 нинг модуль p бўйича тескари қиймати, R_2^{-1} — R_2 нинг модуль p бўйича тескари қиймати, $\backslash\backslash$ — модуль p бўйича $R_1 * R_2$ параметрли даражага ошириш рамзидир.

Мазкур муаммо ҳам R_1, R_2 маълум бўлсагина, Диффи-Хэллман муаммосига келтирилиши мумкин.

4.3 Матрицавий даража параметри муаммосига мос Диффи-Хэллман муаммоси

6-бўлимда келтирилган криптографик тизимларнинг бир қанчасида модуль сифатида туб сондан фойдаланилган бўлиб, уларнинг криптобардошлилиги матрицавий даража параметри муаммосининг мураккаблигига асосланган. Шунингдек, уларнинг баъзиларида махфий асос ва\ёки махфий матрицавий параметр ишлатилган. Матрицавий даража параметри муаммоси матрицавий асос ва матрицавий параметрнинг махфийлигини назарда тутади.

Матрицавий даража параметри ***муаммоси*** қуйидагича таърифланади: агар туб модуль p, $GF_m(p)$ чекли матрицавий майдоннинг mxm тартибли ҳосил қилувчи (генератор) матрицавий элементи $(E+A)$ ва матрицавий параметрли функцияси қиймати $Y \equiv (A \times \underline{R}^{-1})\backslash e \pmod p$ берилган бўлса, тескари матрицаси мавжуд бўлган матрицавий параметр $\underline{R}$ ва шу матрицавий параметр билан даражага ошириш даража кўрсаткичи e топилсин, бу ерда $\underline{R}^{-1}$ — $\underline{R}$ нинг модуль p бўйича тескари матрицаси.

Бу муаммонинг юзага келиши криптография коммуникация тизимларини янгича ёндашувлар асосида яратиш имкониятини тугдиради. Муаммони ечиш учун аввало матрицавий пара-

метр $\underline{R}$ ни топиш керак. Ундан сўнг бу муаммони матрицавий дискрет логарифм муаммосига келтириш мумкин. Аммо, матрицавий параметр $\underline{R}$ ни кетма-кет танлаш усули, яъни кучли ҳужум усулидан ўзгача топиш усули ҳозиргача маълум эмас.

Агар матрицавий параметр $\underline{R}$ маълум бўлса, матрицавий даража параметри муаммоси матрицавий дискрет логарифм муаммосига 7, 9-хоссалар асосида қуйидагича келтирилади:

Берилган: $Y \equiv (A \times \underline{R}^{-1})^{\backslash e} (mod\ p)$

$\Downarrow$

$\underline{R}_1^{-1} \times A^{\backslash e} (mod\ p) \equiv (\underline{R}_1^{-1} \times A)^{\backslash\backslash e} (mod\ p)$ (7-хосса, $\underline{R}=E$ учун)

$\Downarrow \underline{R}_1$ ўрнига R қўйиш

$(A \times \underline{R}^{-1})^{\backslash e} (mod\ p) \equiv R^{-1} \times A^{\backslash\backslash e} (mod\ p)$

$\Downarrow$ таққосламани R га кўпайтириш

$\underline{R} \times (A \times \underline{R}^{-1})^{\backslash e} (mod\ p) \equiv A^{\backslash\backslash e} (mod\ p)$

$\Downarrow$ (9-хосса, 2-қисм, $\underline{R}=E$ учун)

$A^{\backslash\backslash e} (mod\ p) \equiv (E+A)^e - E (mod\ p)$

$\Downarrow$ таққосламага E ни қўшиш

$E+A^{\backslash\backslash e} (mod\ p) \equiv (E+A)^e (mod\ p)$

$\Downarrow$ матрицавий дискрет логарифм муаммоси

$E+ \underline{R} \times Y (mod\ p) \equiv (E+A)^e (mod\ p)$.

Матрицавий даража параметри ***муаммоси***: туб p, $GF_m(p)$ ҳосил қилувчи $E+A$ ва $E+\underline{R} \times Y \in GF_m(p)$ элемент берилган, шундай $0 \le e < \varphi_m(p)$ бўлган бутун e сонни топингки, унда $(E+A)^e \equiv E+\underline{R} \times Y (mod\ p)$ бўлсин.

Матрицавий даража параметри муаммоси асосида унга мос матрицавий Диффи-Хэллман муаммоси келиб чиқади.

Матрицавий даража параметри ***муаммосига*** мос ***матрицавий Диффи-Хэллман муаммоси*** қуйидагича таърифланади:

агар туб модуль p, $GF_m(p)$ чекли матрицавий тўпламнинг $m \times m$ тартибли ҳосил қилувчи (генератор) матрицавий элементи $(E+A)$ ва матрицавий параметр $\underline{R}$ билан мос тарзда даражага ошириш функциялари қийматлари

$Y_1 \equiv (A \times \underline{R}^{-1})^{\backslash e} (mod\ p)$, $Y_2 \equiv (A \times \underline{R}^{-1})^{\backslash d} (mod\ p)$ берилган бўлса, $\underline{R}$ ва $((A \times \underline{R}^{-1})^{\backslash e})^{\backslash d} (mod\ p) \equiv ((A \times \underline{R}^{-1})^{\backslash d})^{\backslash e} (mod\ p)$ топилсин, бу ерда

$\underline{R}^{-1}$ — $\underline{R}$ нинг модуль p бўйича тескари матрицаси, $\backslash$ — модуль p бўйича $\underline{R}$ матрицавий параметр билан даражага ошириш рамзидир.

Мазкур муаммо ҳам $\underline{R}$ маълум бўлсагина, матрицавий Диффи-Хэллман муаммосига келтирилиши мумкин.

4-бўлим бўйича хулосалар

1. Параметрли функциянинг 3-синфга оид хоссалари мавжуд муаммолардан мураккаблик поғоналари билан фарқланадиган даража параметри муаммосини ва унга мос бўлган Диффи-Хэллман муаммосини келтириб чикаради. Даража параметрини топиш муаммосига ўхшаш ҳисоблаш мураккаблигига оид муаммо нашрларда келтирилмаган.

2. Агар даража параметри берилган бўлса, унда даража параметри муаммоси дискрет логарифм муаммосига 2.3.8, 2.3.3-хоссалар асосида осонгина келтирилади. Шунингдек, даража параметри муаммосига мос Диффи-Хэллман муаммоси R_1, R_2 маълум бўлсагина, Диффи-Хэллман муаммосига, матрицавий даража параметри муаммосига мос матрицавий Диффи-Хэллман муаммоси эса $\underline{R}$ маълум бўлса, матрицавий Диффи-Хэллман муаммосига келтирилади.

5-БЎЛИМ

ДИАМАТРИЦАЛАР АЛГЕБРАЛАРИГА АСОСЛАНГАН СИММЕТРИК КРИПТОТИЗИМЛАР

Мазкур бўлимда диаматрицалар алгебралари асосида шифрлаш алгоритми ва уни амалга ошириш тартиботлари келтирилган. Симметрик криптотизимга оид ишлаб чиқилган шифр блокли шифр бўлиб, *128* ёки *256* битга каррали узунликка эга бўлган маълумотлар учун мўлжалланган Ўзбекистон Давлат стандартининг [26, 28] такомиллаштирилган русумидир. Уларда диаматрицалар алгебрасининг модуль бўйича қўпайтириш амалидан ва шифрда байтлаб алмаштиришда бир томонлама параметрли функциядан фойдаланилганлиги келтирилган шифрлаш алгоритмини мавжуд криптотизимлардан асосий фарқли томонларини белгилайди. Шифрлаш алгоритми киришида, чиқишида, оралиқ алмаштириш босқичида оралиқ ҳолатлар ва уларни ўзгартириш жараёнида фойдаланиладиган боскич калитлари бир хил ўлчамли массивлардан иборатлигини назарда тутиб, аввало шу массивлар хусусида тўхталиб, сўнгра шифрлаш алгоритми ва уни амалга ошириш тартиботлари ҳақида алоҳида-алоҳида тўхталамиз.

Амалий шифрлаш тартиботи ихтиёрий узунликдаги маълумотларни юқори самарадорлик билан алмаштириладиган бўлиши зарурияти маълумотларни бир хил блокларга бўлиб, ҳар бири устида алмаштиришларни кетма-кет бир неча босқич (раунд) давомида даврий бажариладиган алгоритмлар асосида яратишни тақозо этади.

5.1 Симметрик криптотизимларни диаматрицалар алгебралари асосида яратиш усули

1-бўлимда криптологлар орасида машҳур бўлган DES, ГОСТ, AES, IDEA ва FEAL алгоритмларининг қиёсий таснифлари, шифрларга асосий талаблар, фойдаланиш маромлари

кўрсатиб ўтилган. Шунингдек, уларда фойдаланилган амаллар тўплами модуль арифметикасида бажарилган бўлиб, суриш, иккилик модулда битлаб қўшиш, ўрин алмаштириш ва ўрнига қўйиш (ночизиқли *S*-блок) ўзгартиришларидан фойдаланиш уларнинг барчасига хос экани таъкидлаб ўтилган. Келтирилган алгоритмлар бир-биридан модуль қиймати ва тури билан фарқланиб, фақат AES да полиномли модулдан фойдаланилса, қолган алгоритмларда туб ва/ёки мураккаб модуль бўйича матрицавий қўшиш ва кўпайтириш амалларидан фойдаланилади. IDEAда сонлар устида кўпайтириш амали ночизиқли *S*-блок вазифасини ўтайди.

Симметрик криптотизимларни такомиллашган диаматрицалар алгебраси асосида яратиш усули матрицалар алгебраси асосида шифр-ўзгартишлар ўрнига такомиллашган диаматрицалар алгебрасидан фойдаланишни, шунингдек мавжуд блокли шифрларда фойдаланилаётган кўпайтириш ва тескарилаш амаллари ўрнига элементларни алмаштириш жадвалларини қуришда диаматрица-устунлар алгебраси ҳамда параметрли алгебра амалларидан фойдаланишни назарда тутади [19, 21]. Иккинчи бўлимда кўрсатилганидек, кириш диаматрицасини доимий диаматрицага диаматрицавий кўпайтиришга асосланган шифралмаштиришларда киришда битта элемент ўзгариши, чиқишда матрицавий кўпайтма чиқишидагига нисбатан *1,5-1,75* марта кўп элементларнинг ўзгаришига олиб келиши алмаштириш босқичлари сонини камайтириш имконини беради.

Бу усул асосида, нафақат мавжуд симметрик криптотизимларни алгебраик амаллар аналогиясидан фойдаланиб, улардан кам бўлмаган криптобардошлиликка эга бўлган, уларга ўхшаш криптотизимлар яратиш мумкин, балки махфий параметрлардан турлича фойдаланиш асосида, мавжуд симметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар яратиш имкониятини яратади.

Симметрик криптотизимларни диаматрицалар алгебралари (такомиллашган диаматрицалар ва диаматрица-устунлар алгебралари ҳамда параметрли алгебра) асосида яратиш усули криптотизим яратиш усулига асосий прототип танлашдан, прототипда фойдаланилган чекли бутун сонлар тўплами

устида берилган матрицалар ва матрица-устунлар тўпламлари устида матрицавий қўшиш +, матрицавий кўпайтириш х, скалярга кўпайтириш *, матрицавий тескарилаш $^{-1}$, бирлик элементи $\boldsymbol{E}$, ноллик элементи $\boldsymbol{0}$ ни, чекли бутун сонлар майдони устида берилган қўшиш + , кўпайтириш *, тескарилаш $^{-1}$, кўпайтириш амали асосида амалга ошириладиган даража e га ошириш $\uparrow^e$ амалларини ҳамда бирлик элементи 1, ноллик элементи 0 ни такомиллашган диаматрицалар устида бажариладиган диаматрицавий қўшиш +, диаматрицавий кўпайтириш $®_2$, (диаматрица-устунлар алгебрасида параметрли кўпайтириш $®_3$) диаматрицавий тескарилаш $^{-d1}$, бирлик элементи (диаматрицалар алгебраси бирлик элементи $\boldsymbol{E}$, диаматрица-устунлар алгебрасида бирлик элементи $\boldsymbol{0}$), диаматрицавий ноллик элементи $\boldsymbol{0}$, диаматрица-устунлар алгебраси ноллик элементи $\boldsymbol{0}$ билан ва параметрли алгебрада, ўзаро мос тарзда, қўшиш $®_0$ ($R=0$), кўпайтириш ® ($R>0$), тескарилаш $^{\backslash -1}$ ($R>0$), даража e га ошириш $^{\backslash e}$ ($R>0$) амаллари, бирлик элементи 0 ($R>0$) ҳамда ноллик элементи 0 ($R=0$) билан алмаштиришдан, усулни синовдан ўтказишдан иборат.

Мазкур усул симметрик криптотизимлар алгоритмларида анъанавий алгебраларда ўрнатилган амаллар ва элементлар рамзлари сатрини

+	x	$^{-1}$	$\boldsymbol{E}$	$\boldsymbol{0}$	+	*	$^{-1}$	$\boldsymbol{E}$	$\boldsymbol{0}$	+	*	$^{-1}$	$\uparrow^e$	1	0

ўрнига мос тарзда диаматрицавий ва параметрли алгебраларнинг диаматрицавий параметрли амаллар ва элементлар рамзлари сатри

+	$®_2$	$^{-d1}$	$\boldsymbol{E}$	$\boldsymbol{0}$	+	$®_3$	$^{-d1}$	$\boldsymbol{0}$	$\boldsymbol{0}$	$®_0$	®	$^{\backslash -1}$	$^{\backslash e}$	0	0

билан алмаштириб, криптотизим параметрлари тўпламига қўшимча тарзда, камида битта параметр $R>0$ белгилашдан ҳамда усулни синовдан ўтказишдан иборат [19, 21].

Бу ерда иккала сатрда ҳам $\uparrow^e$ ни $^{\backslash e}$ га алмаштиришда бутун сонли даража кўрсаткичлари бир хил эканлигини унутмаслик лозим. Бинобарин, усул прототипда фойдаланилган даража кўрсаткичларига оид таққосламаларга тегишли бўлмай, ушбу таққосламалар ўзгаришсиз қолади. Даражага ошириш функциясида даража асоси чекли майдонда ҳосил қилувчи-

генератор элемент (бошланғич илдиз) бўлса, уни параметр R бўйича берилган чекли тўпламнинг генератор элементи билан алмаштириш зарур.

5.2 Шифрлаш алгоритмининг кириш ва чиқиш элементлари

[28] ни такомиллаштириш мақсадларида ишлаб чиқилган шифрлаш тартиботида кириш кетма-кетлиги узунлиги *128* ёки *256* битга каррали бўлиб, чиқиш кетма-кетлиги *128* ёки *256* бит этиб белгиланган узунликка эгадир. Ҳар бир блокка тегишли кетма-кетликлардаги битлар нолдан бошлаб кетма-кетлик узунлигидан биттага кам бўлган сонгача тартиб билан рақамланади. Шу билан бирга, битнинг тартиб раками унинг индекси каби маълум бўлган $0 \le i < 128$ ёки $0 \le i < 256$ ораликда ётади.

Изоҳ: бундан буён келтирилган математик ифодаларда, агар кириш ва чикиш блоклари узунлиги *128* битни ташкил этса, у ҳолда $p = 16$ бит ва агар кириш ва чиқиш блоклари узунлиги *256* битни ташкил этса, у ҳолда $p = 256$ бит қабул қилинади.

Шифр тартиботида *128* бит узунликдаги кириш блокларига ишлов бериш учун асосий бирлик бу ярим байт — тўрт битли кетма-кетликдир. Кириш, чиқиш ва босқич калитларининг битлар кетма-кетлигига ярим байт массивлари каби ишлов берилади, ушбу битлар кетма-кетлиги қўшни бўлган тўрт битли кетма-кет гуруҳларга бўлиш йўли билан ҳосил қилинган ярим байтлар массивлари сифатида ишловдан ўтади [28].

a ҳарфи билан белгиланган кириш, чиқиш ёки босқич калити учун натижавий массивдаги ярим байтлар a_n ёки $a[n]$ шаклларининг биридан фойдаланган ҳолда белгиланади, бу ерда n $0 \le n < 32$ ораликда жойлашган.

Ярим байтнинг ҳамма қийматлари унинг якка тартибдаги бит қийматларининг (*0* ёки *1*), қавслар орасида $\{b_3, b_2, b_1, b_0\}$ тартибда конкатенацияси каби ифодаланади.

Шифрлаш тартиботида *256* бит узунликдаги кириш блокларига ишлов бериш учун асосий бирлик бу байт — саккиз бит-

ли кетма-кетликдир. Кириш, чикиш ва боскич калитларининг битлар кетма-кетлигига байт массивлари каби ишлов берилади, ушбу битлар кетма-кетлиги қўшни бўлган саккиз битли кетма-кет гуруҳларга бўлиш йўли билан ҳосил қилинган байтлар массивлари сифатида ишловдан ўтади.

a ҳарфи билан белгиланган кириш, чиқиш ёки босқич калити учун натижавий массивдаги байтларни a_n ёки $a[n]$ шаклларининг биридан фойдаланган ҳолда белгиланади, бу ерда n $0 \le n < 32$ ораликда жойлашган.

Байтнинг ҳамма қийматлари унинг якка тартибдаги бит қийматларининг (*0* ёки *1*), кавслар орасида $\{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}$ тартибда конкатенацияси каби ифодаланади.

Масалан, $\{01100011\}$ байтнинг қиймати учун бит қийматлари $b_7=0$, $b_6=1$, $b_5=1$, $b_4=0$, $b_3=0$, $b_2=0$, $b_1=1$, $b_0=1$ каби ифодаланади.

5.3 Holat(holat) ва Holatn(holatn) массивлари

Шифрлаш алгоритмида маълумотларни қайта ишлаш жараёнини ярим байтлар (байтлар)дан тузилган икки ўлчамли *Holat* массиви устида алгоритм амалларини бажариш деб қараш мумкин [28].

Holat массиви саккизта сатр (қатор) ва тўртта устунда жойлашган ярим байтлардан (байтлардан) иборат, бунда ҳар бир сатр *32* (*64*) битдан иборат.

h билан белгиланган *Holat* массивида ҳар бир алоҳида олинган ярим байт (байт) иккита *s* ва *u* индексга эга, бу ерда *s* — сатрнинг $0 \le s < 8$ ораликдаги қиймати; *u* — устуннинг $0 \le u < 4$ ораликдаги қиймати. Ушбу индекслаш *Holat* массивининг аниқ бир ярим байтига (байтига) *h* [*s, u*] каби ҳавола қилиш имконини беради.

Шифрлаш жараёни, биринчи бўлимда келтирилган маълум шифрлар каби, беш асосий маромда фойдаланишга мўлжалланган.

Электрон код китоби маромида шифрлаш жараёнида кириш блоклари бири-биридан мустақил шифрланади. Кейинги бандларда келтирилган шифр тартиботи шу маромни назарда

тутади. Бошқа маромлар учун келтирилган шифр тартиботини тўлдириш ҳеч қандай қийинчилик туғдирмайди. Масалан, блокларни илактириш маромида шифрлаш жараёнининг энг бошида (дастлабки матнни шифрматнга айлантиришда) ёки сўнггида (шифрматнни дастлабки матнга айлантиришда) кириш массивининг навбатдаги блоки *kirish* - $кir_0$, kir_1,... kir_{31} — ярим байтлар (байтлар)дан тузилган массивнинг нусхаси *Holatn* массивига кўчирилади. Бу ерда $a_n = kir_n$ белгиланган. Кейин *Holatn* массиви билан аввалги кириш блокини ўзгартириш натижаси устида модуль *2* бўйича қўшиш амалини қўллаш натижасида *Holat* массиви ҳосил бўлади. Сўнгра *Holat* массиви устида навбатдаги босқичга тегишли шифрлаш амаллари бажарилади, ундан кейин *Holat* массиви элементларининг якуний қиймати нусхаси чиқиш массиви *chiqish* — ярим байтлар (байтлар) массиви $chiq_0$, $chiq_1$, ... $chiq_{31}$ га кўчирилади. Бу ерда $a_n = chiq_n$ белгиланган.

Шуни таъкидлаш зарурки, диаматрицалар (ёки диаматрица-устунлар)ни кўпайтириш амалига асосланган алмаштиришлардан олдин икки ўлчамли *Holat* [*8,4*] массивини 5.1-расмда кўрсатилгандек: H_1 [*4,4*] ва H_2 [*4,4*] юқориги ва пастки ярим қисмларга ажратиш керак.

Алмаштиришлар тугагандан сўнг, бу ярим қисмлар нусхалари яна *Holat* [*8,4*] массивига кўчирилади.

H_1 массиви

h1[0,0]	*h1[0,1]*	*h1[0,2]*	*h1[0,3]*
h1[1,0]	*h1[1,1]*	*h1[1,2]*	*h1[1,3]*
h1[2,0]	*h1[2,1]*	*h1[2,2]*	*h1[2,3]*
h1[3,0]	*h1[3,1]*	*h1[3,2]*	*h1[3,3]*

H_2 массиви

h2[0,0]	*h2[0,1]*	*h2[0,2]*	*h2[0,3]*
h2[1,0]	*h2[1,1]*	*h2[1,2]*	*h2[1,3]*
h2[2,0]	*h2[2,1]*	*h2[2,2]*	*h2[2,3]*
h2[3,0]	*h2[3,1]*	*h2[3,2]*	*h2[3,3]*

5.1-расм. H_1 [*4,4*] ва H_2 [*4,4*] массивлари.

5.4 Босқич калити массиви K_e

Шифрлаш жараёнида босқич калитлари массивлари ўзгариб боради. Боскич калити массиви K_e 5.2-расмда кўрсатилганидек,

саккизта сатр ва тўртта устунда жойлашган ярим байтлардан (байтлардан) иборат, массивнинг ҳар бир алоҳида ярим байти (байти)га $K_e[s, u]$ га *Holat* массивидаги каби ҳавола қилиш мумкин.

K_e массиви

$k_e[0,0]$	$k_e[0,1]$	$k_e[0,2]$	$k_e[0,3]$
$k_e[1,0]$	$k_e[1,1]$	$k_e[1,2]$	$k_e[1,3]$
$k_e[2,0]$	$k_e[2,1]$	$k_e[2,2]$	$k_e[2,3]$
$k_e[3,0]$	$k_e[3,1]$	$k_e[3,2]$	$k_e[3,3]$
$ke[4,0]$	$ke[4,1]$	$ke[4,2]$	$ke[4,3]$
$ke[5,0]$	$ke[5,1]$	$ke[5,2]$	$ke[5,3]$
$ke[6,0]$	$ke[6,1]$	$ke[6,2]$	$ke[6,3]$
$ke[7,0]$	$ke[7,1]$	$ke[7,2]$	$ke[7,3]$

5.2-расм. Боскич калити массиви K_e.

Шуни таъкидлаш зарурки, диаматрицалар (ёки диаматрица-устунлар)ни кўпайтириш амалига асосланган алмаштиришлардан олдин икки ўлчамли k_e $[8,4]$ массивини 5.3-расмда кўрсатилгандек, K_{e1} $[4,4]$ ва K_{e2} $[4,4]$ юқориги ва пастки ярим қисмларга ажратиш керак.

K_{e1} массиви

$k_{e1}[0,0]$	k_{e1} $[0,1]$	k_{e1} $[0,2]$	k_{e1} $[0,3]$
k_{e1} $[1,0]$	k_{e1} $[1,1]$	k_{e1} $[1,2]$	k_{e1} $[1,3]$
k_{e1} $[2,0]$	k_{e1} $[2,1]$	k_{e1} $[2,2]$	k_{e1} $[2,3]$
k_{e1} $[3,0]$	k_{e1} $[3,1]$	k_{e1} $[3,2]$	k_{e1} $[3,3]$

K_{e2} массиви

$k_{e2}[0,0]$	k_{e2} $[0,1]$	k_{e2} $[0,2]$	k_{e2} $[0,3]$
k_{e2} $[1,0]$	k_{e2} $[1,1]$	k_{e2} $[1,2]$	k_{e2} $[1,3]$
k_{e2} $[2,0]$	k_{e2} $[2,1]$	k_{e2} $[2,2]$	k_{e2} $[2,3]$
k_{e2} $[3,0]$	k_{e2} $[3,1]$	k_{e2} $[3,2]$	k_{e2} $[3,3]$

5.3-расм. K_{e1} $[4,4]$ ва K_{e2} $[4,4]$ массивлари.

Диаматрицавий (ёки диаматрица-устунлараро) кўпайтиришлар тугагандан кейин бу ярим қисмлар $K_e[8,4]$ массивига нусха кўчирилади.

5.5 Диаматрицалар алгебралари амаллари асосида оддий ва функционал алмаштиришлар

Блокли шифрларни яратишда ҳар қадамда шифрланадиган блок узунлигини танлаш муҳим аҳамиятга эга. Чунки, шифрматнларнинг статистик белгилари блок узунлигига боғлиқ бўлиб, блок узунлиги кам бўлганда статистик криптотаҳлиллаш усулларидан фойдаланиш имконияти пайдо бўлади [76]. Шу сабабли, кўпчилик замонавий шифрлар учун блок узунлиги *64* битдан кам олинмаган. Блок узунлиги ҳаддан зиёд олинганда эса, нафақат криптотаҳлил, балки шифрлаш алгоритми ҳам мураккаблашади. Бу жаҳонда мавжуд компьютерларнинг кўпчилиги *32* битли экани билан боғлиқ. Шифр яратишда суришлар ва энг содда мантиқий амал — *2* модули бўйича битлаб қўшиш амалидан, яъни истисноли ЁКИ амали билан бир қаторда турли амаллардан фойдаланилади. Булар қаторига мазкур бўлимда ёритилган алгебраик амалларни ҳам киритиш қўшимча имкониятларга йўл очади.

Дастлабки матн ва шифрматн блоклари, шифрлаш жараёнида юзага келган оралиқ ҳолатлар *Holat* массивига ёзилади [28].

Шифр учун иккита калитдан — шифрлаш калити k ва функционал калит k_f дан фойдаланилади. Булар ҳар бирининг узунлиги бўйича дастлабки матн узунлигига мос тарзда *128* ёки *256* бит олинади. Натижада, уч хил *128*, *256* ва *512* бит калит узунликларидан фойдаланилади. Биринчи ҳолда, *128* бит калит шифрлаш калити k бўлиб, у дастлабки сеансда функционал калит k_f шифрлаш калити k нинг хэш-қиймати сифатида ҳисобланади. Иккинчи ҳолда кириш блоклари *128* бит бўлса, *256* битнинг биринчи ярми шифрлаш калити k, иккинчи ярми функционал калит k_f бўлиб хизмат қилади, агар кириш блоклари *256* бит бўлса, унда *256* бит калит шифрлаш калити k бўлиб, у дастлабки сеансда функционал калит k_f шифрлаш калити k нинг хэш-қиймати сифатида ҳисобланади. Учинчи ҳолда кириш блоклари *256* бит бўлиб, *512* битнинг биринчи ярми шифрлаш калити k, иккинчи ярми функционал калит k_f бўлиб хизмат қилади. Барча ҳолларда функционал калит k_f сеанслар

гуруҳи учун янгиланиб боради. Бунда жорий сеанс гуруҳи учун янгиланган функционал калит k_f аввалги сеанс гуруҳига тегишли функционал калит k_{f-1} нинг хэш-қиймати сифатида ҳисобланади. Хэшлаш калити сифатида қоида тарзида шифрлаш калити k дан фойдаланилади. Функционал калит k_f ни янгилаш даври (YA) ахборотни муҳофазалаш даражаси билан белгиланади. Масалан, $1 \le YA < 100$ бўлиши мумкин. Ахборотни муҳофазалаш даражаси энг юқори бўлганда функционал калит k_f ҳар сеансда янгиланиб туради.

Шифрлаш жараёнида шифрлаш сеанси калити массиви K_s ва сеанс давомида шифрлаш босқичи калити массиви K_e дан фойдаланилади. Булар шифрлаш калити k ва функционал калит k_f асосида шакллантирилади.

Шифрда фойдаланилган оддий шифралмаштиришлар ва калитлар билан боғлиқ алмаштиришлар қуйида келтирилган. Улар ҳаммаси бўлиб *8* та алмаштиришдан иборат бўлиб, уларнинг бештаси *Holat* массиви устида бажарилади, *4* таси дастлабки матн блоклари узунлигига мос тарзда ярим байт ёки байт сатҳида, биттаси байт сатҳида бажарилади. Қолганлари шифрлаш сеанси учун калитлар массивини ва ҳар босқич учун босқич калити массивини шакллантиришга хизмат қилади.

Маълумотларни шифрлаш алгоритми қуйидаги параметрлардан фойдаланади [28]:

a) k — *128*, *256* ёки *512* бит узунликдаги шифрлаш калити;

b) k_f — *128* ёки *256* бит узунликдаги шифрлаш калити;

c) K_e — *8* x *4* тартибли икки ўлчамли массив шаклидаги босқич калити;

d) b — *128* ёки *256* битли кириш блоклари сони;

e) e — босқичлар сони *128* битли кириш блоклари учун *10-14* оралиғида, *256* битли блоклар учун *6-8* оралиғида;

f) p, $(p+1)$ — модуль, $p \in \{16, 256\}$;

Маълумотларни шифрлаш алгоритми қуйидаги функциялардан фойдаланади:

a) *Aralash*() — оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштириш учун диаматрица ёки диаматрица-устунга тегишли қисмлари устида амалга оширилади; бунда *Holat* массивининг ҳар бир диаматри-

цавий (ёки диаматрица-устунга тегишли) кисмини ўнгдан аралаштириш диаматрицаси (ёки аралаштириш диаматрица-устун қисми)га кўпайтириш амалидан фойдаланилади; аралаштириш диаматрицаси (ёки аралаштириш диаматрица-устун қисми) *Holat* массивининг ҳар бир диаматрицавий (ёки аралаштириш диаматрица-устун) қисми учун турли бўлиб, сеанс-босқич калити массиви k_{sb} нинг ҳар хил қисми асосида шакллантирилган махсус тузилмали диаматрица (ёки аралаштириш диаматрица-устун қисми)дан иборат бўлади; мазкур шифралмаштириш кириши *Holat* массиви, тўғри ва тескари аралаштириш диаматрица ёки тўғри ёки тескари аралаштиришнинг диаматрица-устун кисмларига бўлиб, чиқиши *Holat* массивидир;

b) *BaytAlmash*() — оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* массиви элементларини алмаштириш массиви элементлари билан байт сатҳида алмаштириш учун фойдаланилади; мазкур шифралмаштириш кириши байт сатҳида *Holat* массиви, алмаштириш массивлари k_s, k_{so} бўлиб, чиқиши байт сатҳида *Holat* массивидир;

c) *Sur*() — *Holat* массиви элементларини янада яхшироқ аралаштириш учун, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда фойдаланилади; мазкур алмаштириш кириши ярим байт (байт) сатҳида *Holat* массиви, чиқиши устун бўйлаб шифрлашда пастга ва сатр бўйлаб ўнгга ёки шифрни очишда устун бўйлаб юқорига ва сатр бўйлаб чапга сурилган ярим байт (байт) сатҳида *Holat* массивидир;

d) *Qo'shBosqichKalit*() — оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* ва босқич калити массиви K_e элементлари устида истисноли ЁКИ (*2* модули бўйича битлаб қўшиш) амалини бажаришдан иборат; мазкур шифралмаштириш кириши ярим байт (байт) сатҳида *Holat* массиви, K_e массиви бўлиб, ярим байт (байт) сатҳида *Holat* массивидир;

e) *ShaklSeansKalitBayt* () — сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *BaytAlmash*() шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши

шифрлаш калити k ва функционал калит k_f бўлиб, чиқиши бир ўлчамли бит сатҳида сеанс-босқич калити массиви k_{se} ва бир ўлчамли байт сатҳида чизиқли алмаштиришлар массивлари k_s, k_{so} дир. k_s, k_{so} массивларини ҳосил қилишда, бир томонлама параметрли функциядан фойдаланилади; бир томонлама параметрли функцияда параметр, асос ва даража кўрсаткичи сифатида чизиқли сеанс-босқич калити массиви k_{sb} нинг уч байтли қисми олинади;

f) *ShaklSeansKalit* () — сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Aralash*() шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши шифрлаш калити k ва функционал калит k_f бўлиб, чиқиши икки вариантдан бирида амалга оширилади:

биринчи вариантда шифралмаштириш чиқиши шифрматнни шакллантириш маромида икки ўлчамли диаматрица-устун қисмларидан иборат *8x4* ўлчамли сеанс калитининг массиви K_{ss} бўлса, дастлабки матн шакллантириш маромида икки ўлчамли K_{ss} га тескари диаматрица-устун қисмларидан иборат *8x4* ўлчамли сеанс калитининг массиви K_{ssi} дир;

иккинчи вариантда шифралмаштириш чиқиши шифрматн ва дастлабки матн шакллантириш маромларида икки ўлчамли тўғри ва тескари махсус тузилмали диаматрицалардан иборат *4x4* ўлчамли сеанс калитининг массивлари K_s, K_{so} дир;

g) *ShaklBosqichKalit*() — сеанс давомида сеанс-босқич калитидан босқич калити массивлари K_{bs}, K_{bso} ни шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Qo'shBosqichKalit*() алмаштиришини бажариш учун фойдаланилади; мазкур алмаштириш кириши чизиқли сеанс-босқич калити массиви k_{se}, чиқиши икки ўлчамли босқич калити массивлари K_{bs}, K_{bso} дир.

h) *Qo'shHolat*() — оддий шифралмаштириш бўлиб, шифрлаш блокларни электрон код китоби маромидан бошқа маромларда дастлабки матнни шифрматнга ва тескари йўналишда *XOR* амали иштирокида фойдаланиладиган алмаштириш.

5.6 Шифрнинг псевдокоди

Шифрлаш криптографик модулини ишга туширишда (5.4-расм) аввало шифрлаш калити k ва функционал калит k_f ўрнатилган босқичлар сони e модулга юкланади. Шунингдек, дастлабки матнни шифрматнга алмаштириш маромида дастлабки матн, шифрматнни дастлабки матнга алмаштириш маромида эса шифрматн модулининг *Holat* массивига юкланади. Шифрлаш жараёнининг бошланишида *ShaklSeansKalitBayt*(k,k_f), *ShaklSeansKalit*(k,k_f) ва *ShaklBosqichKalit*(k_{se}) ишга туширилади, натижада байт сатҳида алмаштириш массивлари, аралаштириш диаматрица-устун (ёки аралаштириш диаматрица) қисмларидан таркиб топган сеанс калити массивлари ва алмаштириш массивлари шакллантирилади. Бу массивлар токи k, k_f лар ўзгармас бўлиб қолар экан, кейинги сеансларда ҳам фойдаланилаверади.

Электрон код китоби маромида кейинги жараёнлар шифрнинг псевдокодида келтирилган тартибда шифрлаш йўналишига $m \in \{s, s_o\}$ боғлиқ тарзда босқичлар сони e давомида содир бўлади. Бу ерда s — дастлабки матнни шифрматнга алмаштириш йўналишини, s_o — шифрматнни дастлабки матнга алмаштириш йўналишини белгилайди. Ҳар босқичда *Aralash*(*Holat*, K_s), *BaytAlmash*(*Holat*, K_b), *Qo'shBosqichKalit*(*Holat*, K_b), *Sur*(*Holat*), *ShaklBosqichKalit*(k_{sb}) оддий алмаштиришларидан фойдаланилади. Бу ерда *Qo'shBosqichKalit*(*Holat*, K_e) ва *Sur* (*Holat*) энг содда амаллардир.

e та босқич давомида, даврий жараёнлардан сўнг *Aralash* (*Holat*, K_s), *Qo'shBosqichKalit*(*Holat*, K_b) оддий шифралмаштиришлари амалга оширилгач *Holat* массиви чиқиш массивига, яъни дастлабки матнни шифрматнга алмаштириш йўналишида шифрматнга, шифрматнни дастлабки матнга алмаштириш йўналишида эса, дастлабки матнга алмашади.

```
Shifr (byte kirish [32], byte chiqish [32], byte k[32] , byte kf[32])
(byte kirish [320], byte chiqish [32], byte k[32], bit b[4], bit e[3])
begin
        byte ke [4,8], Ks [4,8], Kb [4,8]
        Holat [4,8],  Holatn[4,8]
        ke= k
        Holatn = kirish
        Holat = 0
        ShaklSeansKalitBayt (k, kf)
        ShaklSeansKalit(k, kf)
        ShaklBosqichKalit(ksb)

        for  blok =0 step 1 to b-1
            Qo'shHolat(Holatn, Holat)
            Holat = Holatn
          for  bosqich =1 step 1 to e - 1
            if m=s then    Qo'shBosqichKalit(Holat, Kb)
                  else         Aralash(Holat, Ks)      end if
                     if m=s then    Aralash(Holat, Ks)
                  else       Qo'shBosqichKalit(Holat, Kb)   end if
                     if m=s then     Sur(Holat)
                  else       ShaklBosqichKalit(ksb)       end if
        ByteAlmash(Holat, Kb)
              if m=s then     ShaklBosqichKalit(ksb)
                 else      Sur(Holat)                    end if
        end for
              if m=s then    Qo'shBosqichKalit(Holat, Kb)
                else        Aralash(Holat, Ks)          end if
              if m=s then     Aralash(Holat, Ks)
                else    Qo'shBosqichKalit(Holat, Kb)   end if
        chiqish= Holat
end
```

5.4-расм. Шифрнинг псевдокоди.

Aralash(*Holat*, K_s), *ByteAlmash*(*Holat*, K_b), *Qo'shBosqich-Kalit*(*Holat*, K_b), *Sur*(*Holat*) оддий шифралмаштиришлари ва

ShaklSeansKalitBayt(k,k_f), *ShaklSeansKalit*(k, k_f), *ShaklBosqich-Kalit*(k_{sb}) алмаштиришлари кейинги бандда келтирилган.

Шифр модулининг дастурий-аппаратли шаклида функционал калит янгилаш жараёнини *ShaklSeansKalitBayt*(k,k_f), *ShaklSeansKalit* (k, k_f) алмаштириш жараёнлари билан қўшиб олиб бориш мақсадга мувофиқдир. Унда шифр тартиботига *ShaklSeansKalitBayt*(k,k_f), *ShaklSeansKalit* (k, k_f) натижаларини киритиш назарда тутилиши лозим.

5.7 Шифрнинг алмаштиришлари

5.7.1 *ShaklSeansKalitBayt*(k,k_f) алмаштириши

ShaklSeansKalitBayt(k,k_f) алмаштириши қуйидаги амалларни бажаришдан иборат:

5.7.1.1 $k_{se} = k + k' * (1 + k_f * k)$ ҳисоблансин ва чапдан *336* (*672*) бит қолдирилсин, бунда $k' - k_f$ нинг ўнгдан *96* (*192*) битли қисми.

5.7.1.2 k_{se} да ўнгдан *128+24* (*256+24*) битли қисм ажратиб олинсин, чапдан *128* (*256*) битли қисмдан ярим байт (байт)ли элементлардан таркиб топган чизиқли массив K_{st}=[*0,1,2,3,... 31*], қолган *24* битли қисмдан — байт сатҳида элементлардан таркиб топган чизиқли массив K_{shh}= [*0,1,2*] шакллантирилсин.

5.7.1.3 Чизиқли массив K_{shh}=[*0,1,2*] элементларидан қуйида келтирилган қоидалар асосида *s, R, L* параметрлари шакллантирилсин:

1) *j=0* учун агар $k_{shh}[j] < 3$ бўлса, *s=3* қабул қилинсин, акс ҳолда $s = k_{shh}[0]$ қабул қилинсин.

2) *j=1* учун, агар $k_{shh}[j] = 0$ бўлса, *R=1* қабул қилинсин, акс ҳолда $R = k_{shh}[1]$ қабул қилинсин.

3) *j=2* учун, агар$_{shh}$[*j*]=*0* бўлса, *L=1* қабул қилинсин, акс ҳолда $L = k_{shh}[2]$ қабул қилинсин.

4) *s* (*mod 2*)=*0* учун, агар *s* (*mod 4*)=*0* бўлса, *s=s-1* қабул қилинсин, акс ҳолда *s=s+1* қабул қилинсин.

5) *s* (*mod 2*)=*1* учун, агар *s-1* (*mod 4*)=*0* бўлса, у ҳолда *s=s-2* қабул қилинсин.

5.7.1.4 Байт сатҳида алмаштириб шифрматн ҳосил қилиш учун, бир ўлчамли массив K_{sh} [*256*] шакллантирилсин.

Бунинг учун ҳар бир $i \in \{0,1,2,...255\}$ га мос $i+L$ қийматни s даражага параметр R билан 257 модули бўйича оширилсин, натижа 256 модули бўйича тақдим этилсин ва ҳар қадамда натижа i билан таққослансин. Агар таққосланган қийматлар тенг бўлса, у ҳолда $s \equiv s+4$ $(mod256)$ қабул қилинсин ва ҳисоблашлар қайтадан бажарилсин.

Ҳисоблашлар алгоритми қуйидаги амалларни ўз ичига олади:

1) $i=0$ қабул қилинсин.

2) $k_{sh}[i] \equiv ((i+L)(mod256))^s (mod\ 257)(mod\ 256)$ ҳисоблансин.

Токи $i<256$ гача, агар $i==k_{sh}[i]$ бўлса, у ҳолда $s \equiv s+4$ $(mod256)$ қабул қилинсин ва *1*-қадамга қайтилсин, акс ҳолда $i=i+1$ қабул қилинсин va *2*- қадамга қайтилсин.

3) $k_{sh}[i,\ i=0,1,2,...255]$ элементларидан байт сатҳида алмаштириб шифрматн ҳосил қилиш учун чизиқли массив K_{sh} $[256]$ шакллантирилсин.

5.7.1.5 Байт сатҳида алмаштириб шифр очиш учун чизиқли массив K_{sho} $[256]$ шакллантирилсин.

Бунинг учун байт сатҳида алмаштириб шифрматн ҳосил қилиш учун чизиқли массив K_{sh} $[256]$да ҳар бир элемент $k_{sh}[i]$ ни унинг манзили (индекси)га тенг қийматга алмаштириш ва ҳосил бўлган массивни манзиллар ортиб бориши тартибида жойлаштириш қифоя.

5.7.2 ShaklSeansKalit (k, k_f) алмаштириши

ShaklSeansKalit (k, k_f) алмаштириши *икки вариантдан бирида* амалга оширилади.

Биринчи вариантда ShaklSeansKalit (k, k_f) алмаштиришини амалга ошириш қуйидаги амалларни бажаришдан иборат:

5.7.2.1 Ярим байт (байт)ли элементлардан таркиб топган чизиқли массив $K_{st}=[0,1,2,3,...\ 31]$ учун

1-қадам: $1+R \equiv k_{st}[0].+k_{st}[1].+....+k_{st}[31](mod\ p)$ ҳисоблансин, агар $1+R(mod\ 2)=0$ бўлса, у ҳолда $K_{st}=[0,1,2,3,...\ 31]$ да $k_{st}[31]=k_{st}[31]-1$ қўйилсин ва *1*-қадамга қайтилсин.

2-қадам: $K_{st}=[0,1,2,3,...\ 31]$ асосида $8x4$ тартибли K_{ss} массиви шакллантирилсин.

Массив K_{st}

$k_{st}[0]$	$k_{st}1[1]$	$k_{st}[2]$	$k_st[3]$
$k_{st}[4]$	$k_{st}[5]$	$k_{st}[6]$	$k_{st}[7]$
$k_{st}[8]$	$k_{st}[9]$	$k_{st}[10]$	$k_{st}[11]$
$k_{st}[12]$	$k_{st}[13]$	$k_{st}[14]$	$k_{st}[15]$
$k_{st}[16]$	$k_{st}[17]$	$k_{st}[18]$	$k_{st}[19]$
$k_{st}[20]$	$k_{st}[21]$	$k_{st}[22]$	$k_st[23]$
$k_{st}[24]$	$k_{st}[25]$	$k_{st}[26]$	k_{st} 127]
k_{st} 128]	k_{st} 129]	$k_{st}[30]$	k_{st} 131]

Массив K_{ss}

$k_{ss}[0,0]$	$k_{ss}[0,1]$	$k_{ss}[0,2]$	$k_{ss}[0,3]$]
$k_{ss}[1,0]$	$k_{ss}[1,1]$	$k_{ss}[1,2]$	$k_{ss}[1,3]$]
$k_{ss}[2,0]$	$k_{ss}[2,1]$	$k_{ss}[2,2]$	$k_{ss}[2,3]$]
k_{ss} [30]	$k_{ss}[3,1]$	$k_{ss}[3,2]$	$k_{ss}[3,3]$]
$k_{ss}[4,0]$	$k_{ss}[4,1]$	$k_{ss}[4,2]$	$k_{ss}[4,3]$]
$k_{ss}[5,0]$	$k_{ss}[5,1]$	$k_{ss}[5,2]$	$k_{ss}[5,3]$]
$k_{ss}[6,0]$	$k_{ss}[6,1]$	$k_{ss}[6,2]$	$k_{ss}[6,3]$]
$k_{ss}[7,0]$	$k_{ss}[7,1]$	$k_{ss}[7,2]$	$k_{ss}[7,3]$]

3-қадам: $(1+R)_t \equiv (1+R)^{-1} (mod\ p)$ ҳисоблансин.

4-қадам: $8x4$ тартибли K_{ss} массивининг ҳар бир элементи $k_{ss}[i,j]$ учун $k_{ss}[i,j] \equiv k_{ss}[i,j]*(1+R)_t\ (mod\ p)$ ҳисоблансин, бу ерда $i=0,...7,\ j=0,...3$ ва улардан $8x4$ тартибли K_{sst} массив шакллантирилсин.

Массив K_{sst}

$k_{sst}[0,0]$	$k_{sst}[0,1]$	$k_{sst}[0,2]$	$k_{sst}[0,3]$]
$k_{sst}[1,0]$	$k_{sst}[1,1]$	$k_{sst}[1,2]$	$k_{sst}[1,3]$]
$k_{sst}[2,0]$	$k_{sst}[2,1]$	$k_{sst}[2,2]$	$k_{sst}[2,3]$]
k_{sst} [30]	$k_{ss}[3,1]$	$k_{ss}[3,2]$	$k_{ss}[3,3]$]
$k_{sst}[4,0]$	$k_{sst}[4,1]$	$k_{sst}[4,2]$	$k_{sst}[4,3]$]
$k_{sst}[5,0]$	$k_{sst}[5,1]$	$k_{sst}[5,2]$	$k_{sst}[5,3]$]
$k_{sst}[6,0]$	$k_{sst}[6,1]$	$k_{sst}[6,2]$	$k_{sst}[6,3]$]
$k_{sst}[7,0]$	$k_{sst}[7,1]$	$k_{sst}[7,2]$	$k_{sst}[7,3]$]

5.7.3 *Aralash* (*Holat*) алмаштириши

Aralash(*Holat*) алмаштириши икки вариантда амалга оширилади.

Биринчи вариантда Aralash(*Holat*) алмаштириши қуйидаги амалларни бажаришдан иборат:

Агар *ms=s* бўлса, унда *Holat* $\circledR_3 K_{ss}$ (*mod p*)ни ҳисобланг, натижани *Holat* массивига кўчиринг, бу ерда $\circledR_3$ диаматрица-устунлар алгебрасида параметр *R* билан кўпайтириш рамзи.

Ҳисоблашлар қуйидаги қадамлар кетма-кетлигини амалга оширишдан иборат:

Holat массиви учун параметр

$R \equiv h[0,0]+ h[0,1]+ h[0,3]+ h[1,0]+...+ h[7,2]+ h[7,3]$ (*mod p*) ни ҳисобланг.

$i=0,...7, j=0,...3$ учун $h[i,j] \equiv h[i,j] + (1+R)* k_{ss}[i,j]$ (*mod p*)ни ҳисобланг ва натижани *Holat* массивига кўчиринг.

Агар *ms=sh* бўлса, у ҳолда *Holat* $\circledR_3 K_{sst}$ (*mod p*)ни ҳисобланг, натижани *Holat* массивига кўчиринг.

Ҳисоблашлар қуйидаги қадамлар кетма-кетлигини амалга оширишдан иборат:

1) *Holat* массиви учун параметр

$R \equiv h[0,0]+ h[0,1]+ h[0,3]+ h[1,0]+...+ h[7,2]+ h[7,3]$ (*mod p*) ни ҳисобланг.

2) K_{ss} массиви учун параметр

$R_s \equiv k_{ss}[0,0]+ k_{ss}[0,1]+ k_{ss}[0,3]+ k_{ss}[1,0]+...+ k_{ss}[7,2]+ +k_{ss}[7,3]$ (*mod p*) ни ҳисобланг.

3) $i=0,...7, j=0,...3$ учун $h[i,j] \equiv h[i,j] + (1+R)* k_{sst}[i,j]$ (*mod p*) ни ҳисобланг ва натижани *Holat* массивига кўчиринг; бу ерда $k_{sst}[i,j] \equiv - (1+R_s)^{-1} * k_{ss}[i,j]$ (*mod p*).

Мазкур алмаштириш ўзининг юқори тезкорлиги билан характерланади, унда матрицани скалярга кўпайтиришга нисбатан аралаштириш натижаси максимал эффективликка эга. Чунки, *Holat* массивининг битта элементи ўзгарган бўлса, қайси элемент ўзгарган бўлишидан қатъий назар, диаматрица-устунлараро кўпайтириш оқибатида бу барча элементнинг ўзгаришига олиб келади.

Иккинчи вариантда Aralash(*Holat*) алмаштириши қуйидаги амалларни бажаришдан иборат:

агар $ms=s$ бўлса, унда $K_1=K_{1t}$, $K_2=K_2$ қабул қилинсин, H_1 ®$_2$ K_1 $(mod\ p)$, H_2 ®$_2$ K_{s2} $(mod\ p)$ ҳисоблансин, натижа H_1, H_2 массивларига ёзилиб, *Holat* массивига кўчирилсин, акс ҳолда, яъни $ms=sh$ бўлса, унда $K_1=K_{1t}$, $K_2=K_{2t}$ қабул қилинсин, H_1®$_2$ $K_1(mod p)$, H_2 ®$_2$ K_2 $(mod\ p)$ ҳисоблансин, натижа H_1, H_2 массивларига ёзилиб, *Holat* массивига кўчирилсин.

®$_2$ амали қуйида келтирилган ифодалар асосида ҳисобланади ва бунда ифодалардаги остки индекс $s\in\{1,2\}$ олинади.

$i=j\in\{0,1,2,3\}$ учун ифодалар:

$h'_s[0,0]=h_s[0,0]*(k_s[0,0]+k_s[1,0]+k_s[2,0]+k_s[3,0])-h_s[1,1]*$
$*k_s[1,0]-h_s[2,2]*k_s[2,0]-h_s[3,3]*k_s[3,0](mod\ p)$,

$h'_s[1,1)=h_s[1,1]*(k_s[0,1]+k_s[1,1]+k_s[2,1]+k_s[3,1])-h_s[0,0]*$
$*k_s[0,1]-h_s[2,2]*k_s[2,1]-h_s[3,3]*k_s[3,1](mod\ p)$,

$h'_s[2,2)=h_s[2,2]*(k_s[0,2]+k_s[1,2]+k_s[2,2]+k_s[3,2])-h_s[0,0]*$
$*k_s[0,2]-h_s[1,1]*k_s[1,2]-h_s[3,3]*k_s[3,2](mod\ p)$,

$h'_s[3,3)=h_s[3,3]*(k_s[0,3]+k_s[1,3]+k_s[2,3]+k_s[3,3])-h_s[0,0]*$
$*k_s[0,3]-h_s[1,1]*k_s[1,3]-h_s[2,2]*k_s[2,3](mod\ p)$.

$i\neq j\in\{0,1,2,3\}$ учун ифодалар:

$h'_s[0,1]=h_s[0,1]*(k_s[0,1]+k_s[1,1]+k_s[2,1]+k_s[3,1])+(h_s[0,0]+$
$+h_s[1,0]+h_s[2,0]+h_s[3,0])*k_s[0,1]-h_s[0,2]*k_s[2,1]-h_s[0,3]*k_s[3,1]$
$(mod\ p)$,

$h'_s[0,2]=h_s[0,2]*(k_s[0,2]+k_s[1,2]+k_s[2,2]+k_s[3,2])+(h_s[0,0]+$
$+h_s[1,0]+h_s[2,0]+h_s[3,0])*k_s[0,2]-h_s[0,1]*k_s[1,2]-h_s[0,3]*$
$*k_s[3,2]$ $(mod\ p)$,

$h'_s[0,3]=h_s[0,3]*(k_s[0,3]+k_s[1,3]+k_s[2,3]+k_s[3,3])+(h_s[0,0]+$
$+h_s[1,0]+h_s[2,0]+h_s[3,0])*k_s[0,3]-h_s[0,1]*k_s[1,3]-h_s[0,2]**k_s$
$[2,3]$ $(mod\ p)$,

$h'_s[1,0]=h_s[1,0]*(k_s[0,0]+k_s[1,0]+k_s[2,0]+k_s[3,0])+(h_s[0,1]+$
$+h_s[1,1]+h_s[2,1]+h_s[3,1])*k_s[1,0]-h_s[1,2]*k_s[2,0]-h_s[1,3]**k_s$
$[3,0]$ $(mod\ p)$,

$h'_s[1,2]=h_s[1,2]*(k_s[0,2]+k_s[1,2]+k_s[2,2]+k_s[3,2])+(h_s[0,1]+$
$+h_s[1,1]++h_s[2,1]+h_s[3,1])*k_s[1,2]-h_s[1,0]*k_s[0,2]-h_s[1,3]**k_s$
$[3,2]$ $(mod\ p)$,

$h'_s[1,3]=h_s[1,3]*(k_s[0,3]+k_s[1,3]+k_s[2,3]+k_s[3,3])+(h_s[0,1]+$
$+h_s[1,1]+h_s[2,1]+h_s[3,1])*k_s[1,3]-h_s[1,0]*k_s[0,3]-h_s[1,2]**k_s$
$[2,3]\ (mod\ p)$,

$h'_s[2,0]=h_s[2,0]*(k_s[0,0]+k_s[1,0]+k_s[2,0]+k_s[3,0])+(h_s[0,2]+$
$+h_s[1,2]+h_s[2,2]+h_s[3,2])*k_s[2,0]-h_s[2,1]*k_s[1,0]-h_s[2,3]*$
$*k_s[3,0]\ (mod\ p))$,

$h'_s[2,1]=h_s[2,1]*(k_s[0,1]+k_s[1,1]+k_s[2,1]+k_s[3,1])+(h_s[0,2]+$
$+h_s[1,2]+h_s[2,2]+h_s[3,2])*k_s[2,1]-h_s[2,0]*k_s[0,1]-h_s[2,3]*$
$*k_s[3,1]\ (mod\ p)$,

$h'_s[2,3]=h_s[2,3]*(k_s[0,3]+k_s[1,3]+k_s[2,3]+k_s[3,3])+(h_s[0,2]+$
$+h_s[1,2]+h_s[2,2]+h_s[3,2])*k_s[2,3]-h_s[2,0]*k_s[0,3]-h_s[2,1]**k_s$
$[1,3]\ (mod\ p)$,

$h'_s[3,0]=h_s[3,0]*(k_s[0,0]+k_s[1,0]+k_s[2,0]+k_s[3,0])+(h_s[0,3]+$
$+h_s[1,3]+h_s[2\ 3]+h_s[3,3])*k_s[3,0]-h_s[3,1]*k_s[1,0]-h_s[3,2]**k_s$
$[2,0]\ (mod\ p)$,

$h'_s[3,1]=h_s[3,1]*(k_s[0,1]+k_s[1,1]+k_s[2,1]+k_s[3,1])+(h_s[0,3]+$
$+h_s[1,3]+h_s[2,3]+h_s[3,3])*k_s[3,1]-h_s[3,0]*k_s[0,1]-h_s[3,2]**k_s$
$[2,1]\ (mod\ p)$,

$h'_s[3,2]=h_s[3,2]*(k_s[0,2]+k_s[1,2]+k_s[2,2]+k_s[3,2])+(h_s[0,3]+$
$+h_s[1,3]+h_s[2,3]+h_s[3,3])*k_s[3,2]-h_s[3,0]*k_s[0,2]-h_s[3,1]**k_s$
$[1,2]\ (mod\ p)$.

Мазкур алмаштиришда матрицавий кўпайтиришга нисбатан аралаштириш натижаси эффективрокдир. Чунки *Holat* массивининг битта элементи ўзгарган бўлса, қайси элемент ўзгарган бўлишига қараб, диаматрицавий кўпайтириш оқибатида бу *6* ёки *7* тагача элементнинг ўзгаришига олиб келади.

5.7.4 *BaytAlmash* (*Holat*) алмаштириши

BaytAlmash (*Holat*) алмаштириши қуйидаги амалларни бажаришдан иборат.

1) Элементлари ярим байт (байт) сатҳида берилган *Holat*[*8, 4*] массиви элементлари байт сатҳида берилган *Holatb*[*4, 4*] массивига алмаштирилсин.

2) Агар *ms=s* бўлса, у ҳолда $K_a = K_{sh}$ [*256*] қабул қилинсин, *Holatb*[*4, 4*] массивининг ҳар бир элементи K_a массивининг адреси бўйича унга мос элементи билан алмаштирилсин ва натижавий *Holatb*[*4, 4*] массиви ярим байт сатҳида берилган *Holat*[*8, 4*] массивига алмаштирилсин, акс ҳолда, яъни *ms=sh* бўлса, у ҳолда $K_a = K_{sho}$ [*256*] қабул қилинсин, *Holatb*[*4, 4*] массивининг ҳар бир элементи K_a массивининг адреси бўйича унга мос элементи билан алмаштирилсин ва натижавий *Holatb*[*4, 4*] массиви ярим байт сатҳида берилган *Holat*[*8, 4*] массивига алмаштирилсин.

5.7.5 *ShaklBosqichKalit* (k_{se}) алмаштириши

ShaklBosqichKalit (k_{se}) алмаштириши босқич бошлангунча (*e<1*) ва босқич давомида (*e≥1*) бир-биридан фарқли тарзда қуйидаги усулда шакллантирилади:

1) *e<1* ва *ms=s* бўлса, у ҳолда чизиқли сеанс-босқич калити массиви k_{se} ўзгармай қолсин, агар *e<1* ва *ms=sh* бўлса, у ҳолда даврий тарзда чапга k_{se} массиви *336* (*672*) — *e* x*41*(*83*) битга сурилсин.

Чизиқли сеанс-босқич калити массивининг чап томонидан *128* (*256*) битли қисмини ажратиб олиб, ундан элементлари ярим байт сатҳида берилган K_e[*8,4*] массиви шакллантирилсин.

2) Агар *e≥1* ва *ms=s* бўлса, унда даврий тарзда ўнгга k_{se} массиви *41* (*83*) битга сурилсин, агар *e≥1* ва *ms=sh* бўлса, унда даврий тарзда чапга k_{se} массиви *41* (*83*) битга сурилсин.

Чизиқли сеанс-босқич калити массивининг чап томонидан *128* (*256*) битли қисмини ажратиб олиб, ундан элементлари ярим байт(байт) сатҳида берилган K_e[*8,4*] массиви шакллантирилсин.

5.7.6 *Qo'shBosqichKalit* (*Holat*, K_e) алмаштириши

Qo'shBosqichKalit (*Holat*, K_e) алмаштириши *Holat* ва K_e[*8,4*] массивларининг ҳар бир ярим байт (байт) сатҳдаги бир номли

элементлари устида истисноли ЁКИ (*2* модули бўйича битлаб қўшиш) амалини бажаришдан иборат.

$0 \le c < 8$ учун:

$[h'[c,0], h'[c,1], h'[c,2], h'[c,3]]=[h[c,0], h[c,1], h[c,2], h[c,3]]\oplus$
$\oplus[k_e[c,0], k_e[c,1], k_e[c,2], k_e[c,3]]$.

Натижа *Holat* массивига кўчирилсин.

5.7.7 *Sur* (*Holat*) алмаштириши

Агар $ms=s$ бўлса, унда даврий тарзда *Holat* массивининг биринчи устуни устун бўйлаб пастга ва сатр бўйлаб ўнгга *1* ярим байт (байт)га, иккинчи устуни устун бўйлаб пастга ва сатр бўйлаб ўнгга *2* ярим байт (байт)га, учинчи устуни устун бўйлаб пастга ва сатр бўйлаб ўнгга *3* ярим байт (байт)га сурилсин, акс ҳолда, яъни $ms=sh$ бўлса, унда даврий тарзда устун бўйлаб юқорига ва сатр бўйлаб чапга *Holat* массивининг биринчи устуни *1* ярим байт (байт)га, иккинчи устуни *2* ярим байт (байт)га, учинчи устуни *3* ярим байт (байт)га сурилсин.

5.7.8 *Qo'shHolat*(*Holatn, Holat*) алмаштириши

Qo'shHolat(*Holatn, Holat*) алмаштиришида *Holatn* массивининг ҳар бир ярим байти (байти)га *Holat* массивининг бир номли ярим байт (байти)га оддий битлаб қўшиш *XOR* амали бўйича амалга оширилади (*2* модуль бўйича қўшиш). *Holatn* массиви саккизта яримсўз (сўз) дан иборат. Бу яримсўзлар (сўзлар) $0 \le s < 8$ бўлганда *Holat* массиви устун элементлари алоҳида-алоҳида қуйидагича қўшилади:

$[h'[s,0], h'[s,1], h'[s,2], h'[s,3]]=[h[s,0], h[s,1], h[s,2], h[s,3]]\oplus$
$\oplus [hn[s,0], hn[s,1], hn[s,2], hn[s,3]]$,

бу ерда hn — *Holatn* массиви элементлари, h' — натижавий массив элементлари.

Алмаштириш натижасининг нусхаси *Holat* массивига кўчирилади.

Мазкур бўлимда ишлаб чиқилган маълумотларни шифрлаш тизимидан фойдаланиш учун мўлжалланган протоколлар 2-иловада келтирилган.

Муаллиф раҳбарлигида ишлаб чиқилган Е-ҲУЖЖАТ электрон ҳужжатлар алмашиш тизими ва Е-ХАТ ҳимояланган электрон почта тизимида ушбу маълумотларни шифрлаш тартиботи амалга оширилган.

5-бўлим бўйича хулосалар

1. *Таклиф этилган симметрик криптотизимларни диаматрицалар алгебралари (такомиллашган диаматрицалар ва диаматрица-устунлар алгебралари ҳамда параметрли алгебра) асосида яратиш усули* криптотизим яратиш усулига асосий прототип танлашдан, прототипда фойдаланилган чекли бутун сонлар майдони устида берилган матрицалар ва матрица-устунлар тўплами устида матрицавий амалларни такомиллашган диаматрицалар ва диаматрица-устунлар алгебрасининг диаматрицавий амаллари билан, чекли бутун сонлар майдони устида берилган кўпайтириш амали асосида амалга ошириладиган даражага ошириш ва шунга ўхшаш амалларини ва параметрли алгебрада уларга мос параметрли кўпайтириш амали билан ҳамда тўпламларга тегишли бирлик ва ноллик элементларини мос тарзда ўзаро алмаштиришдан иборат. Бу усул, нафақат мавжуд симметрик криптотизимларни алгебраик амаллар аналогиясидан фойдаланиб улардан кам бўлмаган криптобардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд симметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар яратиш имкониятини беради.

2. Криптотизим яратиш усули учун прототип сифатида АҚШ стандарти AES танланган ҳол учун мураккаб модуль учун муаллиф томонидан ишлаб чикилган шифрда кириш диаматрицасини доимий диаматрицага диаматрицавий кўпайтиришга асосланган шифралмаштиришлардан фойдаланилган. Бунда [28] дан фарқли тарзда, матрицалар ўрнига диаматрицалардан ҳамда параметрли алгебрадан фойдаланилади. Мазкур шифралмаштириш киришида битта элемент-

нинг ўзгариши чиқишда матрицавий кўпайтма чиқишидагига нисбатан *1,5-1,75* марта кўп элементлар ўзгаришига олиб келиши алмаштириш босқичлари сонини камайтириш имконини беради.

3. Прототип сифатида аралаштириш матрицаси ва байтни байтга алмаштириш жадвали ошкора бўлган AES танланиб, муаллиф томонидан ишлаб чиқилган шифр прототипдан, шифр ва функционал калитларга қўшимча суратда аралаштириш диаматрицасининг *20* та яримбайт (байт) сатҳида элементларнинг махфийлиги ва уч байтли махфий параметрлар билан берилган байтни байтга алмаштириш массиви махфийлиги дифференциал ва чизиқли таҳлил усулларидан фойдаланишни мураккаблаштиради. Шунингдек, босқич ва сеанс калитлари функционал калит иштирокида яратилиши, шифрлаш калити ва хэш-функция ёрдамида функционал калит янгиланиб туриши прототипга нисбатан мавжуд криптотаҳлил усулларини мураккаблаштиради ва шифр криптобардошлилигини оширишга хизмат қилади.

6-БЎЛИМ

ДИАМАТРИЦА-УСТУНЛАР АЛГЕБРАСИ ВА ПАРАМЕТРЛИ АЛГЕБРАГА АСОСЛАНГАН НОСИММЕТРИК КРИПТОТИЗИМЛАР

6.1 Диаматрица-устунлар алгебраси ва параметрли алгебра асосида носимметрик криптотизимлар яратиш усули

Носимметрик криптотизимларни диаматрица-устунлар алгебраси ва бутун сонли ҳамда матрицавий параметрли алгебра асосида яратиш усули бутун сонли ва матрицавий параметрли функциянинг анъанавий даражага ошириш функцияси хоссаларидан фарқли томонларидан фойдаланишга, уларнинг криптобардошлилиги ва 4-бўлимда уч мураккаблик поғонасида таърифланган даража параметри муаммоларининг мураккаблигига асосланган [19, 20-25,38]. Бу усул асосида, нафақат мавжуд носимметрик криптотизимларни алгебраик амаллар аналогиясидан фойдаланиб улар билан тенг криптобардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд носимметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар яратиш имконияти мавжуд.

Таъриф. Носимметрик криптотизимларни диаматрица-устунлар алгебраси ва бутун сонли параметрли алгебра асосида яратиш усули криптотизим яратиш усулига асосий прототип танлашдан, прототипда фойдаланилган чекли бутун сонлар майдони устида берилган қўшиш +, кўпайтириш *, тескарилаш $^{-1}$, даража e га ошириш $\uparrow^e$ амалларини ҳамда бирлик элементи *1*, ноллик элементи *0* ни мос тарзда диаматрица-устунлар алгебраси ва бутун сонли параметрли алгебрада, ўзаро мос тарзда қўшиш +, устунлараро кўпайтириш $®_3$ ($R>0$), устунни тескарилаш ($^{-1}$), устун бирлик элементи *0*, параметрли қўшиш $®_0$ ($R=0$), кўпайтириш ® ($R>0$), тескарилаш $^{\setminus -1}$ ($R>0$), даража e

га ошириш $\backslash^e$ ($R>0$) амаллари билан ҳамда бирлик элементи 0 ($R>0$), ноллик элементи 0 ($R=0$) билан алмаштиришдан ҳамда усулни синовдан ўтказишдан иборат.

Мазкур усул носимметрик криптотизимлар алгоритмларида анъанавий алгебраларда ўрнатилган амаллар ва элементлар рамзлари сатрини

+	*	$^{-1}$	1	0	+	*	$^{-1}$	$\uparrow^e$	1	0

ўрнига мос тарзда диаматрица-устунлар алгебраси ва бутун сонли параметрли алгебрада ўзаро мос тарзда қўшиш +, устунлараро кўпайтириш $®_3$ ($R>0$), устунни тескарилаш $^{-1}$, устун бирлик элементи 0, қўшиш $®_0$ ($R=0$), кўпайтириш ® ($R>0$), тескарилаш $\backslash^{-1}$, даража e га ошириш $\backslash^e$ ($R>0$) амаллари билан ҳамда бирлик элементи 0 ($R>0$), ноллик элементи 0 ($R=0$) рамзлари сатри

+	$®_3$	$^{-a1}$	0	0	$®_0$	®	$\backslash^{-1}$	$\backslash^e$	0	0

билан алмаштириб, криптотизим параметрлари тўпламига қўшимча тарзда камида битта бутун сонли параметр $R>0$ белгилашдан иборат.

Бу ерда иккала сатрда ҳам $\uparrow^e$ ни $\backslash^e$ га алмаштиришда бутун сонли даража кўрсаткичлари бир хил эканлигини унутмаслик лозим. Бинобарин, усул прототипда фойдаланилган даража кўрсаткичларига оид таққосламаларга тегишли бўлмай, ушбу таққосламалар ўзгаришсиз қолади.

Таъриф. Носимметрик криптотизимларни матрицавий параметрли алгебра асосида яратиш усули криптотизим яратиш усулига бутун сонли параметрли алгебрада яратилган асосий прототип танлашдан, прототипда фойдаланилган параметрли қўшиш $®_0$ ($R=0$), кўпайтириш ® ($R>0$), тескарилаш $\backslash^{-1}$ ($R>0$), даража e га ошириш $\backslash^e$ ($R>0$) амаллари билан ҳамда бирлик элементи 0 ($R>0$), ноллик элементи 0 ($R=0$) билан ва Эйлер пи-функцияси ($\varphi(n)$)ни матрицавий параметрли алгебрада ўзаро мос тарзда матрицавий параметрли қўшиш $\underline{®}_0$ ($\underline{R}=0$), кўпайтириш $\underline{®}$ ($\underline{R}>0$), тескарилаш $\backslash^{-1}$ ($\underline{R}>0$), даража e га ошириш $\backslash^e$ ($\underline{R}>0$) амаллари билан ҳамда бирлик элементи 0 ($\underline{R}>0$),

ноллик элементи *0* ($\underline{R}=0$) билан ва Эйлер пи-функцияси ($\varphi_m(n)$) билан алмаштиришдан ҳамда усулни синовдан ўтказишдан иборат.

Мазкур усул носимметрик криптотизимлар алгоритмларида бутун сонли параметрли алгебраларда ўрнатилган амаллар ва элементлар рамзлари сатрини

$®_0$	®	*0*	$®_0$	⊢I	⊬	$\varphi(n)$

ўрнига мос тарзда матрицавий параметрли алгебра амаллари ва элементлари рамзлари сатри

$\underline{®}_0$	$\underline{®}$	*0*	$\underline{®}_0$	⊢I	⊬	$\varphi_m(n)$

билан алмаштиришдан иборат.

Бу ерда, иккала сатрда ҳам ⊬ рамзи бутун сонли параметр билан бутун сонли даража кўрсаткичига ошириш рамзи эканини унутмаслик лозим. Бинобарин, усул матрицавий параметр билан матрицавий даража кўрсаткичига оширишни назарда тутмайди.

Унда бутун сонли ёки матрицавий параметр ошкора (очиқ) бўлганда мавжуд носимметрик криптотизимлар билан тенг криптобардошлиликка эга криптотизим ҳосил бўлади, бутун сонли ёки матрицавий параметр махфий бўлганда, мавжуд носимметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар ҳосил бўлади. Улар махфий бутун сонли ёки матрицавий параметрлар миқдори билан боғлик тарзда, мавжуд криптотизимлар кўламига нисбатан, кенг кўламга эга бўлади.

Кейинги бандларда криптотизим яратиш усули учун турли прототиплар танланган ҳоллар учун яратилган криптотизимлар ва алгоритмлар келтирилган.

6.2 Шифр яратишга Полиг-Хэллман усулида ёндашув

Маълумки, Полиг-Хэллман криптотизимида [1] шифрлаш модули сифатида туб ёки таркибли сон бўлган махфий модуль n дан, i-томон билан j-томон учун шифрлаш калити сифатида

бир-бирига модуль $\varphi(n)$ бўйича ўзаро тескари махфий бутун сонлар жуфтлиги (k_{1ij}, k_{2ij}) дан фойдаланилади. Бу ерда кириш ва чиқиш блоклари узунлиги модуль узунлигидан кам бўлмайди. Бир томонлама параметрли функциядан фойдаланилганда ҳам шифр модули таркибли ёки туб сон бўлиши мумкин бўлса ҳам, келтирилган мисоллар туб сон учун берилган. Криптография масалаларига оид параметрли функция хоссаларидан фойдаланиш Полиг-Хэллман криптотизимидан тамойилли фарқ этувчи криптотизимлар яратиш имкониятини беради.

6.2.1 Модуль арифметикасининг бир томонлама параметрли функциянинг 1.3.4-хоссасидан фойдаланиш

Математикавий асос сифатида ***параметрли алгебранинг*** бир томонлама параметрли функциясидан фойдаланилганда ***модуль*** туб сон ***p*** махфий ёки ***ошкора*** параметр бўлиб, ***p ошкора*** параметр бўлганда у барча фойдаланувчилар учун умумий параметр бўлиши мумкин. Бундан буён ***модуль p ошкора*** параметр сифатида назарда тутилган. Шунингдек, шифрлаш калити (k_{1ij}, k_{2ij}) i-томон билан j-томон учун алоҳида ва махфий ёки барча томонлар учун умумий ва ошкора бўлиши мумкин. i-томон билан j-томон учун алоҳида бўлиши шарт бўлган махфий параметр R_{ij} дир. Бунда криптотизимнинг криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланмай, махфий параметр R_{ij} ни қўпол куч ёрдамида топиш мураккаблигига асосланади. Шифрда махфий параметр қатнашгани туфайли унча катта бўлмаган модулларда ҳам зарур криптобардошлилик таъминланади. Бу ***параметрли алгебранинг*** бир томонлама параметрли функциясидан фойдаланишга асосланган шифрни Полиг-Хэллман шифридан тамойилли фарқли томонидир.

Шифрда қуйидаги параметрлардан фойдаланилади:

а) p — махфий ёки ошкора модуль, туб сон, бу ерда $p>2^{255}$. Бу соннинг юқори чегараси шифр муайян амалга оширилганда аниқланиши керак;

b) (k_{1j}, k_{2j}) — ёки (k_{1ij}, k_{2ij}) — p ни параметрли функцияга тегишли Эйлер пи-функцияси φ (p) қиймати бўйича бир-бирига тескари бутун сонлар жуфтлиги — шифрнинг махфий ёки ошкора (*k1, k2*) калитлари, бу ерда $1 << k_1, k_2 < p-1$, $1 << |k_1 - k_2|$ ёки $1 << k_{1ij}, k_{2ij} < p-1, 1 << |k_{1ij} - k_{2ij}|$;

c) R_{ij} — тасодифий сон сифатида генерацияланадиган махфий параметр, бу ерда $1 \leq R_{ij} < p$.

Махфий параметр R_{ij} дан шифрлашда одатда биринчи блокни шифрлашда фойдаланилади, бу блок тасодифий сон ёки махфий калит бўлиши мумкин. Кейинги блокларни шифрлаш учун параметр сифатида ундан аввалги блоклар қиймати бўлган сонлардан фойдаланилади. Бундай усул симметрик шифрлардаги блокларни илактириш маромига ўхшаб кетади.

Ташкилий босқичда i-томон фойдаланувчилар гуруҳи учун умумий туб модулни генерациялайди ва уни фойдаланувчиларга ошкор этади. Шунингдек, *i*-томон учлик (R_{ij}, k_{1ij}, k_{2ij}) дан тузилган махфий калитни генерациялайди ва уни ҳимояланган алоқа канали орқали *j*-томонга етказади.

Алоқа сеанси қуйидаги қадамларни ўз ичига олади:

Шифрматнга ўгириш маромида

$n = 1$ учун, $r = R_{ij}$ параметрли

$SM_1 \equiv M_1^{|k1ij} \pmod p$ ҳисобланади.

$n \in \{2, \ldots b\}$ учун, $r = M_{n-1}$ параметр билан

$SM_n \equiv M_n^{\backslash\backslash k1ij} \pmod p$ ҳисобланади.

Дастлабки матнга ўгириш маромида

$n=1$ учун, $r = R_{ij}$ параметр билан

$M_1 \equiv SM_1^{|k2ij} \pmod p$ ҳисобланади.

$n \in \{2, \ldots b\}$ учун, $r = M_{n-1}$ параметр билан

$M_n \equiv SM_n^{\backslash\backslash k2ij} \pmod p$ ҳисобланади.

Бу ерда $|$ — параметр R_{ij} билан дискрет даражага ошириш рамзи,

$\backslash\backslash$ — параметр $r = M_{n-1}$ билан дискрет даражага ошириш рамзи.

6.1-мисол:

Шифрматнга ўгириш										
n	R_{ij}	k_{1ij}	M_1	M_2	M_3	M_4	SM_1	SM_2	SM_3	SM_4
47	7	13	25	26	27	28	46	14	41	12
Дастлабки матнга ўгириш										
n	R_{ij}	k_{2ij}	SM_1	SM_2	SM_3	SM_4	M_1	M_2	M_3	M_4
47	7	39	46	14	41	12	25	26	27	28

Келтирилган схема ўзининг Полиг-Хэллман криптотизимига нисбатан кам бўлмаган криптобардошлиликни таъминлаши билан тавсифланади.

6.2.2 Модуль арифметикасининг бир томонлама дискрет даражага ошириш функциясининг 2.3.5-хоссасидан фойдаланиш

6.2.1 да баён қилинган шифрни яратишда 3-бўлимда келтирилган параметрли функциянинг 1.3.4-хоссасидан фойдаланилган. Агар шифр яратишга Полиг-Хэллман усулида ёндашувда 2.3.5-хосса $(a^{\backslash d1})^{\backslash\backslash d2} \equiv s \ (mod\ n)$, $(s^{\backslash\backslash e2})^{\backslash e1} \equiv a \ (mod\ n)$ дан фойдаланилса, унда шифрда фойдаланиладиган параметрлар рўйхатининг b) ва c) бандларини қуйидагича ўзгартириш лозим:

b) $((k_{d1ij}, k_{d2ij}), (k_{e1ij}, k_{e2ij}))$ — шифрнинг махфий калитлари тўртлиги; бу ерда (k_{d1ij}, k_{d2ij}) — шифрлаш калитлари жуфтлиги, (k_{e1ij}, k_{e2ij}) — шифрни очиш калитлари жуфтлиги бўлиб, k_{d1ij} билан k_{e1ij}, k_{d2ij} билан k_{e2j} параметрли функцияга тегишли Эйлер пи-функцияси $\varphi(p)$ қиймати бўйича бир-бирига тескари бутун сонлар жуфтликларини ҳосил этади;

c) (R_{1ij}, R_{2ij}) — тасодифий сон сифатида генерацияланадиган махфий параметрлар жуфтлиги, бу ерда $1 \le R_{1ij} > R_{2ij} < p$.

Ташкилий босқичда i-томон фойдаланувчилар гуруҳи учун умумий бўлган туб модуль p ни генерациялайди ва уни фойдаланувчиларга ошкор этади. Шунингдек, *i*-томон тўртлик $(R_{1ij}, R_{2ij}, k_{d1ij}, k_{d2ij})$ дан тузилган махфий калитни генерациялайди ва уни ҳимояланган алоқа канали оркали *j*-томонга етказади ва *j*-томон k_{e1ij}, k_{e2ij} калитларни генерациялайди.

Алоқа сеанси 2.3.5-хосса асосида, яъни параметрлар олтилигидан иборат махфий калитдан фойдаланган ҳолда, амалга оширилган юқорида келтирилган қадамларга ўхшаш қадамларни ўз ичига олади. Шифр яратишга Полиг-Хэллман усулига ёндашувда 2.3.5-хоссадан фойдаланиш нисбатан кичик ошкора модулларда ($p \sim 2^{200}$) ҳам етарли криптобардошлиликка эга симметрик шифрлар яратишга имкон беради, чунки иккита ҳар хил параметрдан фойдаланиш криптотизим бардошлилигини кескин суратга оширади.

6.2.3 Бир томонлама матрицавий параметрли функциядан фойдаланиш

Математикавий асос сифатида матрицавий параметрли алгебранинг бир томонлама матрицавий параметрли функциясидан фойдаланилганда модуль p ошкора параметр бўлиб, у барча фойдаланувчилар учун умумий параметр бўлиши мумкин. Бу ерда, махфий матрицавий параметр қатнашгани туфайли, унча катта бўлмаган модулларда ҳам зарур криптобардошлилик таъминланади.

Шифрда қуйидаги параметрлардан фойдаланилади:

a) p — модуль, туб сон, бунда $p > 2^{128}$. Бу соннинг юқори чегараси электрон рақамли имзо алгоритми муайян амалга оширилганда аниқланиши керак;

b) (k_1, k_2) — матрицавий параметрли функцияга тегишли Эйлер пи-функцияси $\varphi_m(p)$ қиймати бўйича бир-бирига тескари бутун сонлар жуфтлиги — шифрнинг махфий калитлари, бу ерда $1 < k_1, k_2 < p^m - 1$;

c) R_{12} — шифрлаш ва шифр очиш учун $m \times m$ тартибли махфий матрицавий параметрлар.

Бу ерда матрицавий параметрлар юқорида келтирилган усулларга ўхшаш тарзда ҳосил қилиниши мумкин. Қуйида икки томон орасида содир бўладиган битта маром тури билан танишиш билан чекланамиз.

Бу маромда иккала матрицавий параметр тенг бўлиб, тасодифий сонлар матрицаси R тенг бўлиб, тасодифий сонлар матрицаси R_{12} сифатида генерацияланади ва махфий сақланади.

Дастлабки матн блокларини шифрматн блокларига, шифрматн блокларини дастлабки матн блокларига алмаштириш қуйидаги ифодалар асосида бажарилади:

Шифрлашда

$n \in \{1,2,... b\}$ учун матрицавий параметр R_{12} билан

$SMn \equiv Mn^{\backslash k1} \pmod p$ ҳисобланади, сўнгра *SM1, SM2,.... SMb-1, SMb* қабул қилувчи томонга жўнатилади.

Шифр очишда

$n \in \{1,2,... b\}$ учун матрицавий параметр R_{12} билан

$Mn \equiv SMn^{\backslash k2} \pmod p$ ҳисобланади.

Бу ерда *Mn* — *mxm* тартибли дастлабки матн блоқлари, *SMn* — *mxm* тартибли шифрматнблоклари, $n \in \{1,2,... b\}$;

$^{\backslash}$ — матрицавий параметр R_{12} билан даражага ошириш рамзи.

Келтирилган маром ўзининг Полиг-Хэллман криптотизимига нисбатан юқори криптобардошлилик таъминлашлари билан тавсифланади. Бунда, матрицавий параметрнинг тартиби қанча юқори бўлса, шунга мос тарзда шифрнинг криптобардошлилиги шунчалик юқори бўлади. Бу ўз навбатида, унча катта бўлмаган модуллардан фойдаланиб, зарур криптобардошлиликни таъминлашга имконият яратади.

6.3 Шифр яратишга RSA усулида ёндашув

Маълумки, RSA криптотизимида [45-50] шифрлаш модули сифатида махфий иккита (ва ундан ортиқ) хар хил туб сонларнинг кўпайтмаси бўлган мураккаб модуль *n* дан, шифрлаш калити сифатида бир-бирига *n* нинг Эйлер пи-функцияси $\varphi(n)$ қиймати бўйича ўзаро тескари бўлган, биринчиси ошкора, иккинчиси махфий бутун сон бўлган жуфтликдан фойдаланилади. Кириш ва чиқиш блоклари узунлиги модуль узунлигидан кам бўлмайди. Математик асос сифатида модуль арифметикасининг бир томонлама параметрли функциясидан фойдаланилади, бунда 3-бўлимда келтирилган бир томонлама параметрли функция хоссаларининг 1-синфига оид, яъни анъанавий даражага ошириш функциясининг хоссаларига аналог хоссалардан фойдаланиш етарлидир.

Мақсад фақат шифрдан фойдаланиш бўлганда, биринчи томон шифрловчи, t — томон шифр очувчи вазифасини бажаради. Бунда t — томон ўз модулига эга бўлиб, биринчи томон ўз модулига эга бўлмаса ҳам t — томонга унинг модули ва ошкора калитидан фойдаланган ҳолда ахборотни шифрлаб жўнатиш имкониятига эга бўлади. Қуйида шундай ҳол назарда тутилади. Лекин шифрни очиш имкониятига эга бўлиш учун ҳар бир фойдаланувчи ўз модули ва ошкора-махфий калитлар жуфтига эга бўлиши зарур. Бу ҳол электрон рақамли имзога оид бўлимда қаралади.

6.3.1 Шифр яратишда бир томонлама дискрет даражага ошириш функцияси ўрнига *параметрли алгебранинг* бир томонлама параметрли функциясидан фойдаланиш

Шифрда қуйидаги параметрлардан фойдаланилади:

n — модуль, бу ерда $n=p_1 * p_2$, p_1, p_2 — t-томон генерациялаган ҳар хил махфий туб сонлар, p_1, $p_2 > 2^{255}$. Туб сонларнинг юқори чегараси криптотизим муайян амалга оширилганда белгиланиши керак;

(e, d) — n нинг Эйлер пи-функцияси $\varphi(n)$ қиймати бўйича ўзаро тескари бутун сонлар жуфтлиги, e — шифрнинг ошкора калити, d — шифрнинг махфий калити, бу ерда $1 < e, d < \varphi(n)$;

R — шифрлаш ва шифр очиш учун махфий параметр, бу ерда $1 \leq R < n$; параметр R фақат тармоқда қонуний фойдаланувчилар учунгина маълум бўлиб, уни томонларга тарқатиш протоколга биноан амалга оширилади. R дан фойдаланиш камида бешта маромда амалга оширилиши мумкин. Қуйида параметр R дастлабки матннинг ҳар бир блоки учун тенг олинадиган маром билан танишамиз.

Дастлабки матн блокларини шифрматн блокларига, шифрматн блокларини дастлабки матн блокларига алмаштириш қуйидаги ифодалар асосида бажарилади:

1-томонда шифрматнни шакллантиришда

$M_0 M_1$, M_2,.... M_{b-1} учун

R параметр билан $i \in \{0,1,2,\ldots b\text{-}1\}$ учун, $SM_i \equiv M_i^{|et} \ (mod\ n_t)$ ҳисобланади.

$SM_0, SM_1, \ldots SM_{b-1}$, кабул қилувчи t -томонга жўнатилади.

t-томонда шифрматнни дастлабки матнга ўгиришда

R параметр билан $i \in \{0,1,2,\ldots b\text{-}1\}$ учун, $M_i \equiv SM_i^{|dt} (mod\ n_t)$ ҳисобланади,

бу ерда $|$ — параметр R билан дискрет даражага ошириш рамзи.

6.2-мисол

1-томонда шифрматнни шакллантириш

n_1	e_1	R	M_0	M_1	M_2	M_3	SM_0	SM_1	SM_2	SM_3
299	71	53	25	26	27	28	275	13	60	64

t-томонда шифрматнни дастлабки матнга ўгириш

n_t	p_t	q_t	$\varphi(n_t)$	d_t	R	SM_0	SM_1	SM_2	SM_3	M_0	M_1	M_2	M_3
299	13	23	264	119	53	275	13	60	64	25	26	27	28

Келтирилган усулда RSA криптотизимига нисбатан параметр R номаълум бўлган томонлар учунгина криптобардошлилик юқори бўлади, R маълум бўлган томонларга нисбатан эса криптобардошлилик RSA криптотизимидаги каби бўлади.

Албатта, келтирилган усул аввалги бандда келтирилгани каби, 2.3.5-хосса $(a^{\backslash\backslash d1})^{\backslash\backslash d2} \equiv s\ (mod\ n)$, $(s^{\backslash\backslash e2})^{\backslash e1} \equiv a\ (mod\ n)$ дан фойдаланилиб ҳам амалга оширилиши мумкин. Бунда, анъанавий криптомодуллардан фойдаланилса, модуль n билан бир қаторда, параметр жуфтлиги (R_1, R_2) фойдаланувчилар гуруҳи учун маълум бўлиши ва даража кўрсаткичлари жуфтлиги (d_1, d_2) — махфий (шахсий), даража кўрсаткичлари жуфтлиги (e_2, e_1) — ошкора бўлиши лозим бўлади. Агар аппаратли махсус криптомодуллардан фойдаланилса криптобардошлилик қонуний ва ноқонуний фойдаланувчилар учун тенг бўлиб, унинг RSA криптотизимига нисбатан кескин ошишига эришилади. Қуйида 2.3.5-хоссадан фойдаланиш асосида КРОМ ва ундан фойдаланувчилар орасида ҳимояланган алоқа канали ҳосил қилишга мўлжалланган криптотизим ҳақида сўз боради.

6.3.2 КРОМ ва ундан фойдаланувчилар орасида ҳимояланган алоқа канали ҳосил қилишга мўлжалланган криптотизим

Ҳимояланган алоқа канали ҳосил қилишда қуйидаги параметрлар фойдаланилади:

a) n — модуль, бу ерда $n = p_1 * p_2$, p_1, p_2 — КРОМ томонидан генерацияланган ҳар хил махфий туб сонлар, $n > 2^{2048}$, p_1, $p_2 > 2^{1024}$. Туб сонларнинг юқори чегараси криптотизим муайян амалга оширилганда белгиланиши керак;

b) (*e, d*) — КРОМ томонидан генерацияланган n нинг Эйлер пи-функцияси $\varphi(n)$ қиймати бўйича ўзаро тескари бутун сонлар жуфтлиги, e — КРОМ нинг ошкора калити, d — КРОМ нинг шахсий махфий калити, бу ерда $1 < e, d < \varphi(n)$;

c) (d_{1i}, d_{2i}, e_{1i}, e_{2i}) — КРОМ томонидан генерацияланган, *i*-фойдаланувчи билан ҳимояланган алоқа канали ҳосил қилишга мўлжалланган шахсий калит, бу ерда (d_{1i}, d_{2i}) ва (e_{1i}, e_{2i}) ўзаро мос суратда Эйлер пи-функцияси $\varphi(n)$ қиймати бўйича бир-бирига тескари бутун сонлар жуфтликлари, $2^{200} \le e_{1i}, e_{2i} < 2^{256}$.

d) (R_{1i}, R_{2i}) — ҳар бир *i*-фойдаланувчи томонидан тасодифий сон сифатида генерацияланадиган махфий параметрлар жуфтлиги, бу ерда $2^{200} \le R_{1i} > R_{2i} < 2^{256}$. Шундай килиб, КРОМ ва *i*-фойдаланувчининг симметрик калити (R_{1i}, R_{2i}, e_{1i}, e_{2i}) КРОМ-нинг шахсий калити (d_{1i}, d_{2i}) асосида ҳимояланган алоқа канали ҳосил бўлади.

Ташкилий босқичда КРОМ фойдаланувчилар гуруҳи учун умумий бўлган модуль n ни ва ошкора калит e ни генерациялайди ва уни фойдаланувчиларга ошкор этади. Шунингдек, *КРОМ* ўз шахсий калити d ни генерациялайди. *КРОМ* хизматларидан ҳар бир *i*-фойдаланувчи жуфтлик (R_{1i}, R_{2i})дан тузилган *симметрик* махфий калитнинг параметрга оид қисмини генерациялайди ва $a_i = ID_1 || R_{1i} || R_{2i}$ ни шахсан *КРОМ* га етказади ёки $R=1$ параметр билан шифрлаб, $s_i \equiv a_i^{\setminus e} (mod\ n)$ ни ҳимояланмаган алоқа канали орқали *КРОМ* га жўнатади. *КРОМ* дешифрлаб $a_i \equiv s_i^{\setminus d} (mod\ n)$ $a_i = ID_1 || R_{1i} || R_{2i}$ ни тиклайди, ID_1 ни фойдаланувчилар рўйхатига

киритади ва бу билан ҳимояланган алоқа каналидан фойдаланиш учун махфий калитлар тўртлиги (d_{1i}, d_{2i}, e_{1i}, e_{2i}) ни генерациялайди, ($ID_i R_{1i}$, R_{2i}, d_{1i}, d_{2i}, e_{1i}, e_{2i}) ҳимояланган маълумотлар базасига ёзиб қўяди. *КРОМ* ($e_{1i} IIe_{2i}$) ни ўз шахсий калити d ва параметр R_{1i} билан $sign_i \equiv (e_{1i} IIe_{2i})^{\backslash\backslash d} (mod\ n)$ кўринишида имзолаб, i-фойдаланувчига жўнатади. i-фойдаланувчи ошкора калит e ва R_{1i} дан фойдаланиб $(e_{1i} IIe_{2i}) \equiv sign_i^{\backslash\backslash e} (mod\ n)$ кўринишида махфий калит (e_{1i}, e_{2i}) ни тиклайди ва ундан жуфтлик (R_{1i}, R_{2i}) орқали *КРОМ* билан маълумотлар алмашишда фойдаланади. Бу ерда, бошқа фойдаланувчилар параметр R_{1i} i-фойдаланувчи ва *КРОМ* нинг симметрик калитининг бир қисми бўлгани туфайли, махфий калит (e_{1i}, e_{2i}) ни тиклай олмайдилир.

Алоқа сеанси 2.3.5-хосса асосида, яъни махфий тўртликлардан иборат махфий калитдан фойдаланган ҳолда амалга оширилган юқорида келтирилган қадамларга ўхшаш кадамларни ўз ичига олади. Бунда i-фойдаланувчи (R_{1i}, R_{2i}, e_{1i}, e_{2i}) дан, *КРОМ* (R_{1i}, R_{2i}, d_{1i}, d_{2i}) дан фойдаланади. Келтирилган усул асосида шакллантирилган ҳимояланган алоқа канали, биринчи навбатда, электрон рақамли имзо бўйича O'z DSt 1092:2005. «Ахборот технологиялари. Ахборотларни криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари» давлат стандартининг ўзига хос протоколларини [100] татбиқ этувчи *КРОМ* лар учун мўлжалланган. Шуни таъкидлаш жоизки, i-фойдаланувчи (R_{1i}, R_{2i}) *КРОМ* га шахсан ўзи топширса, унда алоқа каналининг ҳимояланганлик даражаси, *КРОМ* томонидан ишлатилган модуль n етарли криптобардошлиликка эга бўлмаганда ҳам етарли даражада юқори бўлади.

6.4 Шифр яратишга Тоҳир Ал Жамол усулида ёндашув

Маълумки, Ал Жамол томонидан носимметрик криптография юзага келган даврнинг бошларида [53, 54] таклиф қилинган усулдан ЭРИ яратиш учун ҳам, шифр яратиш учун ҳам фойдаланиш мумкин.

6.4.1 Ал Жамол усулига мос шифр яратишда бир томонлама параметрли функциянинг 1-синфига оид хоссаларидан фойдаланиш

Шифрда қуйидаги параметрлардан фойдаланилади:

a) (*p, a*) — модуль ва асос вазифасида фойдаланиладиган жуфтликдан иборат ошкора параметр; бу ерда p — туб сон, $p>2^{255}$ шартни қаноатлантиради; бу соннинг юқори чегараси криптотизим муайян амалга оширилганда аникланиши керак; $a < p$ — ошкора бутун сонли сон бўлиб, ω нинг $1 \div (p-1)$ оралиқ қийматларида фақат $\omega = (p-1)$ бўлгандагина параметр $R=1$ билан даража қиймати $a^{\omega} \pmod p \equiv 0$ шартни қаноатлантиради;

b)e_i, d_j — алока каналида *i*-, *j*-томонларнинг мос тарзда ўз махфий калитлари, бу ерда $1 \le e_i, d_j < p-1$;

c) r_i, r_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда махфий параметр сифатида фойдаланадиган ўз махфий калитлари, бу ерда $1 \le r_i, r_j < p-1$;

d) r_{ij} — алоқа каналида *i*-, *j*-томонларнинг параметр сифатида фойдаланадиган ўзаро махфий ёки ошкора калити, бу ерда $r_{ij} \equiv r_i + r_j \pmod p$;

e) y_i, y_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда ошкора калитлари, улар умумий маълумотлар базасида сакланиши ёки коммуникация қанали орқали томонлараро айирбошланиши мумкин;

f) k_i, k_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда ҳар алоқа сеансида тасодифий сон сифатида танланадиган махфий сеанс калитлари, бу ерда $1 \le k_i, k_j < p-1$.

i-, *j*-томонларнинг алоқа ўрнатиш жараёни (*p, a*) жуфтлик ва параметр $R = r_{ij}$ маълум саналиб, ташкилий босқичда ошкора калитларни шакллантириш ва алоқа сеансида шифрматн ($s1_j$; $s2_j$) ни шакллантириш ва уларни дастлабки матн *M* билан алмаштириш жараёнлари бўйича қуйидаги қадамларни ўз ичига олади:

ташкилий босқич:

1-қадам: *i*-томон, ўз махфий калитлари e_i, r_i ни тасодифий сонлар сифатида танлаб, параметр $R=r_i$ билан ўз ошкора калити $y_i \equiv (a^* r_i^{-1})^{|ei} (mod\, p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки *j*-томонга жўнатади;

2-қадам: *j*-томон, ўз махфий калитлари d_j, r_j ни тасодифий сонлар сифатида танлаб, параметр $R=r_j$ билан ўз ошкора калити $y_j \equiv (a^* r_j^{-1})^{|dj} (mod\, p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки *i*-томонга жўнатади;

алоқа сеанси:

1-қадам: *j*-томон *i*-томоннинг ошкора калитини олиб, сеанс калити k_j ни танлаб, параметр $R=r_j$ билан $s_{1j} \equiv (a^* r_j^{-1})^{|kj} (mod\ p)$ ва параметр $R=r_j^*(r_{ij}-r_j)$ билан $s_{2j} \equiv M\ XOR\ (y_i^* r_j^{-1})^{\backslash\backslash kj} (mod\ p\ )$ ни ҳисоблайди, сўнгра икки қисмдан иборат шифрматн $(s1_j;\ s2_j)$ ни *i*-томонга жўнатади;

2-қадам: *i*-томон *j*-томоннинг ошкора қалитини қабул қилиб, $y_j^* r_i^{-1} \equiv y_j^* r_i^{-1} (mod\ p)$ ва параметр $R=r_i^*(r_{ij}-r_i)$ билан $M \equiv s_{2j} XOR (s1_j^* r_i^{-1})^{\backslash\backslash ei} (mod\ p)$ ни ҳисоблаб, дастлабки матнни ҳосил қилади .

Модуль *p* фойдаланувчилар гуруҳи учун умумий, асос *a* эса фойдаланувчилар гуруҳи учун бир хил ёки фойдаланувчилар жуфтлари учун ҳар хил бўлиши мумкин.

6.3-мисол:

i-томон

p	r_i	r_i^{-1}	a	$a^* r_i^{-1}$	e_i	y_j	r_{ij}	$r_i^* r_j$	k_i
107	3	36	7	38	13	73	8	15	39
107	101	89	31	84	37	75	30	37	64

j-томон

p	r_j	r_j^{-1}	a	$a^* r_j^{-1}$	d_j	y_i	r_{ij}	$r_i^* r_j$	k_j
107	5	43	7	87	27	60	8	15	39
107	83	49	31	21	31	83	30	37	64

6.4.2 Ал Жамол усулига мос шифр яратишда матрицавий параметрли функция хоссаларидан фойдаланиш

Шифрда қуйидаги параметрлардан фойдаланилади:

a) (p, A) — модуль ва матрицавий асос вазифасида фойдаланиладиган жуфтликдан иборат ошкора параметр; бу ерда p — туб сон, $p>2^{255}$ шартни қаноатлантиради; бу соннинг юқори чегараси криптотизим муайян амалга оширилганда аниқланиши керак; A — mxm тартибли матрицавий асос бўлиб, ω нинг $1 \div \varphi_m(p)$ оралиқ қийматларида, фақат $\omega = \varphi_m(p)$ бўлгандагина, матрицавий параметр $\underline{R}=1$ билан даража қиймати $A^{\omega}(mod p) \equiv 0$ шартни қаноатлантиради;

b) e_i, d_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда ўз махфий калитлари, бу ерда $1 \le e_i, d_j < p^m - 1$;

c) $\underline{R}_{ij}$ — алоқа каналида *i*-, *j*-томонларнинг матрицавий параметр сифатида фойдаланадиган ўзаро махфий калити;

d) Y_i, Y_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда ошкора калитлари, улар умумий маълумотлар базасида сақланиши ёки коммуникация канали орқали томонлараро айирбошланиши мумкин;

e) k_i, k_j — алоқа каналида *i*-, *j*-томонларнинг мос тарзда, ҳар алоқа сеансида тасодифий сон сифатида танланадиган махфий сеанс калитлари, бу ерда $1 \le k_i, k_j < p-1$.

i-, *j*-томонларнинг алоқа ўрнатиш жараёни (p, A) жуфтлик ва матрицавий параметр $\underline{R} = \underline{R}_{ij}$ маълум саналиб, ташқилий босқичда ошкора калитларни шакллантириш ва алоқа сеансида шифрматн $(S_{1j}; S_{2j})$ ни шакллантириш ва уларни дастлабки матн M га алмаштириш жараёнлари бўйича қуйидаги қадамларни ўз ичига олади:

ташкилий босқич:

1-қадам: *i*-томон, ўз махфий калити e_i ни тасодифий сон сифатида танлаб, матрицавий параметр $\underline{R}_{ij}$ билан ўз ошкора калити

$Y_i \equiv (A \times R_{ij}^{-1})^{|e_i|} (mod\ p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки *j*-томонга жўнатади;

2-қадам: *j*-томон, ўз махфий калити d_j ни тасодифий сон сифатида танлаб, матрицавий параметр $\underline{R}_{ij}$ билан ўз ошкора калити

$Y_j \equiv (A \times \underline{R}_{ij}^{-1})^{\backslash dj} (mod\ p)$ ни ҳисоблайди ва уни умумий маълумотлар базасига ёки *i* -томонга жўнатади;

алоқа сеанси:

1-қадам: *j*-томон *i*-томоннинг ошкора калитини олиб, сеанс калитини k_j танлаб, матрицавий параметр $\underline{R} = \underline{R}_{ij}$ билан

$S_{1j} \equiv (A \times \underline{R}_{ij}^{-1})^{\backslash kj} (mod\ p)$ ва

$S_{2j} \equiv M\ XOR\ Y_i^{\backslash kj} (mod\ p)$ ни

ҳисоблайди, сўнгра икки қисмдан иборат шифрматн $(S1_j; S2_j)$ ни *i*-томонга жўнатади;

2-қадам: *i*-томон *j*-томоннинг ошкора калитини қабул қилиб, матрицавий параметр $\underline{R} = \underline{R}_{ij}$ билан $M \equiv S_{2j} XOR\ S_{1j}^{\backslash ei} (mod\ p)$ ни ҳисоблаб, дастлабки матнни тиклайди.

6.5 Махфий калит алмашув алгоритмини яратишга Диффи-Хэллман усули асосида ёндашув

6.5.1 Махфий калит алмашув тизимини яратишда бир томонлама параметрли функция хоссаларидан фойдаланиш

Даража параметри муаммосига мос Диффи-Хэллман муаммосининг ечими икки томон орасида умумий махфий калитни генерациялашга асос бўлиб хизмат қилади:

агар туб модуль *p*, *GF*(*p*) чекли майдоннинг параметр *R=1* билан ҳосил қилувчи (генератор) элементи *a* ва параметрлар R_1, R_2 билан мос тарзда параметрли функциялар қийматлари $y_1 \equiv (a^* R_1^{-1})^{\backslash e} (mod\ p)$, $y_2 \equiv (a^* R_2^{-1})^{\backslash d} (mod\ p)$ берилган бўлса, R_1, R_2 ва $((a^* R_1^{-1})^{\backslash e} * R_2^{-1})^{\backslash\backslash d}\ (mod\ p) \equiv ((a^* R_2^{-1})^{\backslash d} * R_1^{-1})^{\backslash\backslash e}\ (mod\ p)$ топилсин, бу ерда R_1^{-1} — R_1 нинг модуль *p* бўйича тескари қиймати, R_2^{-1} — R_2 нинг модуль *p* бўйича тескари қиймати, $^{\backslash\backslash}$ — модуль *p* бўйича $R_1 * R_2$ параметрли дискрет даражага ошириш рамзидир.

Бу ерда $k \equiv ((a*R_1^{-1})^{\backslash e} * R_2^{-1})^{\backslash d} (mod\, p) \equiv ((a*R_2^{-1})^{\backslash d} * R_1^{-1})^{\backslash e} (mod\ p)$ коммуникация каналида иккала томон учун махфий калит вазифасини, $y_1 \equiv (a*R_1^{-1})^{\backslash e} (mod\, p)$ биринчи томоннинг ошкора калити вазифасини, $y_2 \equiv (a*R_2^{-1})^{\backslash d} (mod\, p)$ иккинчи томоннинг ошкора калити вазифасини ўтайди. Параметр R_1 ва даража кўрсаткичи e дан таркиб топган жуфтлик (R_1, e) биринчи томоннинг махфий калити вазифасини, параметр R_2 ва даража кўрсаткичи d дан таркиб топган жуфтлик (R_2, d) иккинчи томоннинг махфий калити вазифасини ўтайди. Бутун сон a ва туб модуль p дан таркиб топган жуфтлик (a, p) иккала ёки ундан ортиқ томонлар учун умумий ошкора параметрлардир.

$R_1*R_2 \equiv R_1 * R_2\ (mod\ p)$ параметри хам иккала томон учун махфий ёки ошкора калит вазифасида фойдаланилади ва уни томонларга етказиб беришда ишончли учинчи томон иштирок этади.

Махфий калит алмашиш криптотизимида қуйидаги параметрлардан фойдаланилади:

a) (p, a) — модуль ва асос вазифасида фойдаланиладиган жуфтликдан иборат ошкора параметр; бу ерда p — туб сон, $p > 2^{255}$ шартни қаноатлантиради; бу соннинг юқори чегараси криптотизим муайян амалга оширилганда аниқланиши керак; $a < p$ — ошкора натурал сон бўлиб, ω нинг $1 \div (p-1)$ оралиқ қийматларида, фақат $\omega = (p-1)$ бўлгандагина, параметр $R=1$ билан даража қиймати $a^{\backslash\omega}(mod\, p) \equiv 0$ шартни қаноатлантиради;

b) e_i, d_j — калит алмашувчи *i*-, *j*-томонларнинг мос тарзда ўз махфий калитлари, бу ерда $1 \le e_i, d_j < p-1$;

c) r_i, r_j — калит алмашувчи *i*-, *j*-томонларнинг мос тарзда махфий параметр сифатида фойдаланадиган ўз махфий калитлари, бу ерда $1 \le r_i, r_j < p-1$;

d) r_{ij} — калит алмашувчи *i*-, *j*-томонларнинг параметр сифатида фойдаланадиган ўзаро махфий ёки ошкора калити, бу ерда $r_{ij} \equiv r_i + r_j\ (mod\, p)$;

e) y_i, y_j — калит алмашувчи *i*-, *j*-томонларнинг мос тарзда ошкора калитлари, улар умумий маълумотлар базасида сақланиши ёки коммуникация канали орқали томонлараро айирбошланиши мумкин.

Махфий калит алмашиш жараёни (p, a) жуфтлик ва параметр $R= r_{ij}$ маълум саналиб, қуйидаги қадамларни ўз ичига олади:

1-қадам: i-томон, ўз махфий калитлари e_i, r_i ни тасодифий сонлар сифатида танлаб, параметр $R= r_i$ билан ўз ошкора калити

$y_i \equiv (a^* r_i^{-1})^{|ei} (mod\ p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки j-томонга жўнатади ;

2-қадам: j-томон, ўз махфий калитлари d_j, r_j ни тасодифий сонлар сифатида танлаб, параметр $R=r_j$ билан ўз ошкора калити

$y_j \equiv (a^* r_j^{-1})^{|dj} (mod\ p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки i -томонга жўнатади;

3-қадам: j -томон i- томоннинг ошкора калитини қабул қилиб, $y_i^* r_j^{-1} \equiv y_i^* r_j^{-1} (mod\ p)$ ва параметр $R= r_j^*(r_{ij}- r_j)$ билан

$k_j \equiv (y_i^* r_j^{-1})^{\backslash\backslash dj} (mod\ p)$ ни ҳисоблайди;

4-қадам: i -томон j-томоннинг ошкора калитини қабул қилиб, $y_j^* r_i^{-1} \equiv y_j^* r_i^{-1} (mod\ p)$ ва параметр $R= r_i^*(r_{ij}- r_i)$ билан

$k_i \equiv (y_j^* r_i^{-1})^{\backslash\backslash ei} (mod\ p)$ ни ҳисоблайди, бу ерда i-, j-томонларнинг умумий махфий калити $k= k_i = k_j$.

Модуль p фойдаланувчилар гуруҳи учун умумий, асос a эса фойдаланувчилар гуруҳи учун бир хил ёки фойдаланувчилар жуфтлари учун ҳар хил бўлиши мумкин.

6.4-мисол:

i-томон

p	r_i	r_i^{-1}	a	$a^* r_i^{-1}$	e_i	y_j	r_{ij}	$r_i^* r_j$	k_i
107	3	36	7	38	13	73	8	15	39
107	101	89	31	84	37	75	30	37	64

j-томон

p	r_j	r_j^{-1}	a	$a^* r_j^{-1}$	d_j	y_i	r_{ij}	$r_i^* r_j$	k_j
107	5	43	7	87	27	60	8	15	39
107	83	49	31	21	31	83	30	37	64

6.5.2 Махфий калит алмашув тизимини яратишда диаматрица-устунлар алгебрасининг бир томонлама параметрли функциясидан ва калитларни рўйхатга олиш марказларининг хизматларидан фойдаланиш

Криптотизимда қуйидаги параметрлар фойдаланилади:

a) n_1, n_2 — мос тарзда калитларни рўйхатга олиш марказлари КРОМ$_1$, КРОМ$_2$ томонидан модуль сифатида фойдаланадиган ошкора параметрлар, бу ерда $n_1 = p_1 * p_2$, $n_2 = q_1 * q_2$; p_1, p_2, q_1, q_2 — ҳар хил махфий туб сонлар, p_1, p_2, q_1, $q_2 \geq 2^{2048}$. Туб сонларнинг юкори чегараси криптотизим муайян амалга оширилганда белгиланиши керак;

b) (e_1, d_1), (e_2, d_2) — мос тарзда n_1, n_2 нинг Эйлер пи-функциялари $\varphi(n_1)$, $\varphi(n_2)$ қийматлари бўйича ўзаро тескари бутун сонлар жуфтликлари, e_1, e_2 — мос тарзда КРОМ$_1$, КРОМ$_2$ нинг ошкора калитлари, d_1, d_2 — мос тарзда КРОМ$_1$, КРОМ$_2$ нинг махфий калитлари, бу ерда $2^{160} < e_1$, $d_1 < \varphi(n_1)$, $2^{160} < e_2$, $d_2 < \varphi(n_2)$;

c) (*p*, *1*) — модуль ва асос вазифасида фойдаланувчилар томонидан фойдаланиладиган жуфтликдан иборат ошкора параметр; бу ерда p -туб сон, $p \geq 2^{256}$ шартни қаноатлантиради, бу соннинг юқори чегараси криптотизим муайян амалга оширилганда аниқланиши керак; модуль p даража кўрсаткичининг ω нинг $1 \div (p-1)$ оралиқ қийматларида фақат $\omega=(p-1)$ бўлгандагина параметр $R=1$ билан даража қиймати $1^{\omega} \pmod p \equiv 0$ шартни қаноатлантиради;

d) x_t — ҳар бир фойдаланувчининг шахсий махфий калити, бу ерда $\varphi(p) > x_t \geq 2^{160}$, $i \in \{1,2,...t\}$;

1_i, 1_j — фойдаланувчиларнинг ошкора калитлари, бу ерда 1_i, $1_j < p-1$, $i, j \in \{1,2..t\}$.

a_{ij}, a_{ji} — ҳар бир фойдаланувчилар жуфти учун фойдаланувчи томонидан тасодифий сон сифатида генерацияланадиган фойдаланувчилар жуфтининг КРОМ$_1$ ёки КРОМ$_2$ билан ўзаро махфий калитлари, бу ерда a_{ij}, $a_{ji} < p-1$, $i, j \in \{1,2,...t\}$;

R_{1i}, R_{2i} — мос тарзда КРОМ$_1$, КРОМ$_2$ билан фойдаланувчининг ўзаро махфий бўлган ҳар бир фойдаланувчи томонидан

тасодифий сон сифатида генерацияланадиган калитлари, бу ерда $(n_1; R_{1i})=1$, $(n_2; R_{2i})=1$, $p-1> R_{1i}, R_{2i} \geq 2^{160}$, $i \in \{1,2,...t\}$.

Ошкора умумий параметрлар — *n, e, p, 1* берилган ҳолда, $КРОМ_1$ ва $КРОМ_2$ билан фойдаланувчилар орасида ва фойдаланувчилар жуфти учун махфий калитни шакллантириш жараёнлари икки босқичда кечиб, қуйида келтирилган ифодалар асосида бажарилади:

1-босқич

Ҳар бир фойдаланувчи томонидан шахсий махфий калитни генерациялаш учун тасодифий сон сифатида x_i генерацияланади.

$r = 1$ параметрли $1_i \equiv 1^{|xi} (mod\ p)$ ҳисобланади ва бошқа фойдаланувчиларга жўнатилади.

Ҳар бир фойдаланувчи томонидан $КРОМ_1$ва $КРОМ_2$ билан алоқа ўрнатиш учун тасодифий сонлар сифатида R_{1i}, R_{2i} генерацияланади.

Ҳар бир фойдаланувчи $КРОМ_1$ва $КРОМ_2$ учун ўз идентификация маълумотларини ID_i рақамли шаклда тайёрлайди.

$r_{1i} \equiv R_{1i} + ID_i (mod\ n_1)$ ва

$r = r_{1i}$ параметрли $1_{1i} \equiv 1^{\backslash e1} (mod\ n_1)$ ҳисобланади.

$SID_{1i1} \equiv ID_{1i} * 1_{1i} (mod\ n_1)$,

$SR_{1i1} \equiv R_{1i} * 1_{1i} (mod\ n_1)$ ҳисобланади ва SID_{1i1}, SR_{1i1} $КРОМ_1$ га жўнатилади.

$r_{2i} \equiv R_{2i} + ID_i (mod\ n_2)$ ва

$r = r_{2i}$ параметрли $1_{2i} \equiv 1^{\backslash e2} (mod\ n_2)$ ҳисобланади.

$SID_{1i2} \equiv ID_{1i} * 1_{2i} (mod\ n_2)$,

$SR_{2i2} \equiv R_{2i} * 1_2 (mod\ n_2)$ ҳисобланади ва SID_{1i2}, SR_{2i2} $КРОМ_2$ га жўнатилади.

$КРОМ_1$ томонда

$r_{1i} \equiv SR_{1i1} + SID_{1i1} (mod\ n_1)$ ва

$r = r_{1i}$ параметрли $1_{1i} \equiv 1^{\backslash d1} (mod\ n_1)$ ҳисобланади.

$ID_{1i} \equiv SID_{1i1} * 1_{1i} (mod\ n_1)$,

$R_{1i} \equiv SR_{1i1} * 1_{1i} (mod\ n_1)$ ҳисобланади ва хотирада сақлаб қўйилади.

КРОМ$_2$ томонда

$r_{2i} \equiv SID_{1i2} + SR_{2i2} \ (mod\ n_2)$ ва

$r = r_{2i}$ параметрли $1_{2i} \equiv 1^{\backslash d2} \ (mod\ n_2)$ ҳисобланади.

$ID_{1i} \equiv SID_{1i2} * 1_{2i} \ (mod\ n_2)$,

$R_{2i} \equiv SR_{2i2} * 1_{2i} \ (mod\ n_2)$ ҳисобланади ва хотирада сақлаб қўйилади.

2-босқич

i-томонда

a_{ij} тасодифий сон сифатида генерацияланади.

$R = R_{1i}$ параметрли $Sa_{ij} \equiv a_{ij}^{\backslash\backslash e1} \ (mod\ n_1)$ ҳисобланади ва КРОМ$_1$га жўнатилади.

j-томонда

a_{ji} тасодифий сон сифатида генерацияланади.

$r = R_{2j}$ параметрли $Sa_{ji} \equiv a_{ji}^{\backslash\backslash e2} \ (mod\ n_2)$ ҳисобланади ва КРОМ$_2$-га жўнатилади.

КРОМ$_1$ да калит тасдиқлашда

$r = R_{1i}$ параметрли

$a_{ij} \equiv Sa_{ij}^{\backslash\backslash d1} \ (mod\ n_1)$,

$r = R_{1j}$ параметрли

$SSa_{ij} \equiv a_{ij}^{\backslash\backslash d1} \ (mod\ n_1)$ ҳисобланади ва *j*-томонга жўнатилади.

КРОМ$_2$ да калитни тасдиқлашда

$r = R_{2j}$ параметрли

$a_{ji} \equiv Sa_{ji}^{\backslash\backslash d2} \ (mod\ n_2)$,

$r = R_{2i}$ параметрли

$SSa_{ji} \equiv a_{ji}^{\backslash\backslash d2} \ (mod\ n_2)$ ҳисобланади ва *i*-томонга жўнатилади.

i-томонда махфий калитни шакллантиришда

1) $r = R_{2i}$ параметрли

$a_{ji} \equiv SSa_{ji}^{\backslash\backslash e2} \ (mod\ n_2)$ ҳисобланади.

$R = 1$ параметрли

$1_{ij} \equiv 1_j^{\backslash xi} \ (mod\ p)$ ҳисобланади.

2) $r_{ij} \equiv a_{ij} * a_j \ (mod\ p)$ ҳисобланади.

$r_{ijt} \equiv r_{ij}^{-1} \ (mod\ p)$ ҳисобланади.

$k_{ij} \equiv 1_{ij} * r_{jit} \ (mod\ p)$ ҳисобланади.

Агар k_{ji} икки томонлама келишилган калитларга қўйиладиган талабларга жавоб берса, k_{ij} томонларнинг ўзаро махфий калити сифатида қабул қилинади, акс ҳолда $a_{ij} = a_{ij}+1$ қўйилади ва *2)* қадамга қайтилади.

j-томонда махфий калитни шакллантиришда

1) $r = R_{1j}$ параметрли

$a_{ij} \equiv SSa_{ij}^{\backslash\backslash e1} \ (mod\ n_1)$ ҳисобланади.

$r = 1$ параметрли

$1_{ji} \equiv 1_i^{\backslash xj} \ (mod\ p)$ ҳисобланади.

2) $r_{ji} \equiv a_{ji} * a_{ij} \ (mod\ p)$ ҳисобланади.

$r_{jit} \equiv r_{ji}^{-1} \ (mod\ p)$ ҳисобланади.

$k_{ji} \equiv 1_{ji} * r_{jit} \ (mod\ p)$ ҳисобланади.

Агар k_{ji} икки томонлама келишилган калитларга қўйиладиган талабларга жавоб берса, k_{ji} томонларнинг ўзаро махфий калити сифатида қабул қилинади, акс ҳолда $a_{ij} = a_{ij}+1$ қўйилади ва *2)* қадамга қайтилади.

6.5-мисол

1-босқич

i-томонда

p	ID_i	x_i	R_{1i}	R_{2i}	$1_i = 1^{\backslash xi}$	n_1	e_1	r_{1i}	$1^{\backslash\backslash e1}$	SID_i	SR_{1i}
107	400	63	7	31	45	527	413	407	409	230	228

n_2	e_2	r_{2i}	$1^{\backslash\backslash e2}$	SID_i	SR_{2i}
437	317	431	416	340	223

j-томонда

p	ID_j	x_j	R_{1j}	R_{2j}	$1_j = 1^{\backslash xj}$	n_1	e_1	r_{1j}	$1^{\backslash\backslash e1}$	SID_j	SR_{1j}
107	410	57	13	41	90	527	413	423	69	359	370

n_2	e_2	r_{2j}	$1^{\backslash\backslash e2}$	SID_j	SR_{2j}
437	317	14	410	292	204

$KPOM_1$ томонда

n_1	p_1	p_2	$\varphi(n_1)$	d_1	r_{1i}	$1^{\backslash\backslash d1}$	ID_i	R_{1i}	r_{1j}	$1^{\backslash\backslash d1}$	ID_j	R_{1j}
527	17	31	480	437	458	460	400	7	202	443	410	13

$KPOM_2$ томонда

n_2	q_1	q_2	$\varphi(n_2)$	d_2	r_{2i}	$1^{\backslash\backslash d2}$	ID_i	R_{2i}	r_{2j}	$1^{\backslash\backslash d2}$	ID_j	R_{2j}
437	19	23	396	401	126	104	400	31	59	178	410	41

2-босқич

i-томонда

p	R_{1i}	a_{ij}	n_1	e_1	$Sa_{ij}=a_{ij}^{\backslash\backslash e1}$
107	7	37	527	413	282

j-томонда

p	R_{2j}	a_j	n_2	e_2	$Sa_{ji}=a_{ji}^{\backslash\backslash e2}$
107	41	29	437	317	376

$KPOM_1$ да калитни тасдиқлаш

n_1	p_1	p_2	$\varphi(n_1)$	d_1	R_{1i}	$a_{ij}=Sa_{ij}^{\backslash\backslash d1}$	R_{1j}	$SSa_{ij}=a_{ij}^{\backslash\backslash d1}$
527	17	31	480	437	7	37	13	364

$KPOM_2$ да калитни тасдиқлаш

n_2	q_1	q_2	$\varphi(n_2)$	d_2	R_{2j}	$a_{ji}=Sa_j^{\backslash\backslash d2}$	R_{2i}	$SSa_{ji}=a_{ji}^{\backslash\backslash d2}$
437	19	23	396	401	41	29	31	289

i-томонда махфий калитни шакллантириш

p	x_i	l_j	$l_{ij}\equiv l_j^{\backslash xi}$	n_2	e_2	R_{2i}	a_{ij}	a_{ji}	r_{ij}	r_{iji}	$k_{ij1}\equiv l_{ij} * r_{iji}$
107	63	90	65	437	317	31	37	29	3	36	93

a_{ij}	r_{ij}	r_{iji}	$k_{ij2}\equiv l_{ij} * r_{iji}$
38	32	36	99

j-томонда махфий калитни шакллантириш

p	x_j	l_i	$l_{ji} \equiv l_i^{\setminus xj}$	n_1	e_1	R_{1j}	a_{ji}	a_{ij}	r_{ji}	r_{jit}	$k_{ji1} \equiv l_{ji} * r_{jit}$
107	57	45	65	527	413	13	29	37	3	36	93

a_{ij}	r_{ji}	r_{jit}	$k_{ji2} \equiv l_{ji} * r_{jit}$
38	32	36	99

Бу ерда:

$^{\setminus}$ — параметр $r = 1$ билан дискрет даражага ошириш рамзи, $^{\setminus\setminus}$— параметр R_{1i}, R_{1j}, R_{2i} R_{2j}, r_{1i}, r_{1j}, r_{2i}, ёки r_{2j} билан дискрет даражага ошириш рамзи. $k_{ji1} = 93$ талабга жавоб бермаганда $k_{ji2} = 99$ қабул этилган.

Махфий калитни олдиндан ўзаро келишилган талабга мослаб олиш, бу криптотизимнинг афзалликларидандир.

6.5.3 Махфий калит алмашув тизимини яратишда матрицавий параметрли функциянинг хоссаларидан фойдаланиш

Матрицавий даража параметри муаммосига мос Диффи-Хэллман муаммосининг мавжудлиги икки томон орасида умумий махфий калитни генерациялашга асос бўлиб хизмат қилади.

Матрицавий параметрли функция муаммосига мос Диффи-Хэллман муаммоси қуйидагича таърифланади:

агар туб модуль p, $GF_m(p)$ чекли матрицавий тўпламнинг mxm тартибли ҳосил қилувчи (генератор) матрицавий элементи $(E+A)$ ва матрицавий параметр $\underline{R}$ билан мос тарзда даражага ошириш функциялари қийматлари $Y_1 \equiv (A \times R^{-1})^{\setminus e} \ (mod\ p)$, $Y_2 \equiv (A \times \underline{R}^{-1})^{\setminus d} \ (mod\ p)$ берилган бўлса, $\underline{R}$ ва $((A \times \underline{R}^{-1})^{\setminus e})^{\setminus d} \ (mod\ p) \equiv$ $\equiv ((A \times \underline{R}^{-1})^{\setminus d})^{\setminus e} \ (mod\ p)$ топилсин, бу ерда $\underline{R}^{-1}$ — $\underline{R}$ нинг модуль p бўйича тескари матрицаси, $^{\setminus}$— модуль p бўйича $\underline{R}$ матрицавий параметр билан даражага ошириш рамзидир.

Бу ерда $K \equiv ((A \times \underline{R}^{-1})^{\setminus e})^{\setminus d} \ (mod\ p) \equiv ((A \times \underline{R}^{-1})^{\setminus d})^{\setminus e} \ (mod\ p)$ коммуникация каналида иккала томон учун махфий калит вазифасини,

$Y_1 \equiv (A \times \underline{R}^{-1})^{\backslash e} \pmod{p}$ биринчи томоннинг ошкора калити вазифасини, $Y_2 \equiv (A \times \underline{R}^{-1})^{\backslash d} \pmod{p}$ иккинчи томоннинг ошкора калити вазифасини ўтайди. Даража кўрсаткичи e биринчи томоннинг махфий калити, даража кўрсаткичи d иккинчи томоннинг махфий калити вазифаларини ўтайди. $m \times m$ тартибли матрицавий элемент A ва туб модуль p дан таркиб топган жуфтлик (A, p) иккала ёки ундан ортиқ томонлар учун умумий ошкора параметрлардир.

$m \times m$ тартибли матрицавий параметр $\underline{R}$ иккала томон учун ўзаро махфий калит вазифасида фойдаланилади ва уни томонларга етказиб беришда ишончли учинчи томон ёки ҳимояланган алоқа канали иштирок этади.

Махфий калит алмашиш криптотизимида қуйидаги параметрлардан фойдаланилади:

a) (p, A) — модуль ва матрицавий асос вазифасида фойдаланиладиган жуфтликдан иборат ошкора параметр; бу ерда p — туб сон, $p > 2^{255}$ шартни қаноатлантиради; бу соннинг юқори чегараси криптотизим муайян амалга оширилганда аниқланиши керак; A — $m \times m$ тартибли матрицавий асос бўлиб, ω нинг $1 \div \varphi_m(p)$ оралиқ қийматларида фақат $\omega = \varphi_m(p)$ бўлгандагина матрицавий параметр $R=1$ билан даража қиймати $A^{\backslash \omega} \pmod{p} \equiv 0$ шартни қаноатлантиради;

b) e_i, d_j — калит алмашувчи i-, j-томонларнинг мос тарзда ўз махфий калитлари, бу ерда $1 \leq e_i, d_j < \varphi_m(p)$;

c) $\underline{R}_{ij}$ — калит алмашувчи i-, j-томонларнинг матрицавий параметр сифатида фойдаланадиган ўзаро махфий калити;

d) Y_i, Y_j — калит алмашувчи i-, j-томонларнинг мос тарзда ошкора калитлари, улар КРОМ маълумотлар базасида сақланиши ёки коммуникация канали орқали томонлараро айирбошланиши мумкин.

Махфий калитни алмашиш жараёни (p, A) жуфтлик ва матрицавий параметр $\underline{R}=\underline{R}_{ij}$ маълум саналиб, қуйидаги қадамларни ўз ичига олади:

1-қадам: i-томон, ўз махфий калити e_i ни тасодифий сон сифатида танлаб, матрицавий параметр $\underline{R}_{ij}$ билан ўз ошкора калити $Y_i \equiv (A \times \underline{R}_{ij}^{-1})^{\backslash ei} \pmod{p}$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки j-томонга жўнатади;

2-қадам: j-томон ўз маҳфий калити d_j ни тасодифий сон сифатида танлаб, матрицавий параметр $\underline{R}_{ij}$ билан ўз ошкора калити $Y_j \equiv (A x \underline{R}_{ij}^{-1})^{|dj} \ (mod\ p)$ ни ҳисоблайди ва уни КРОМ маълумотлар базасига ёки i-томонга жўнатади;

3-қадам: j-томон i-томоннинг ошкора калитини қабул қилиб, матрицавий параметр $\underline{R} = \underline{R}_{ij}$ билан $K_j \equiv Y_i^{\wedge dj} \ (mod\ p)$ ни ҳисоблайди;

4-қадам: i-томон j-томоннинг ошкора калитини қабул қилиб, матрицавий параметр $\underline{R} = \underline{R}_{ij}$ билан $K_i \equiv Y_j^{\wedge ei} \ (mod\ p)$ ни ҳисоблайди, бу ерда i-, j-томонларнинг умумий махфий калити $K = K_i = K_j$.

Модуль p ва матрицавий асос A фойдаланувчилар гуруҳи учун бир хил бўлиши мумкин.

6.6-мисол: Бу ерда $p=3$, $p^4-1=80$, $e_i=57$, $d_j=63$.

A				$\underline{R}$				$\underline{R}^{-1}$				$A x \underline{R}^{-1}$			
1	0	1	2	2	1	0	1	1	2	2	1	0	1	0	0
0	2	1	1	1	0	1	2	2	2	1	0	0	0	2	1
2	1	1	2	0	2	1	0	2	2	2	0	0	2	0	1
0	0	1	2	0	1	2	1	0	0	1	1	2	2	1	2

Y_j				Y_i				K_i				K_j			
0	2	1	2	2	1	2	1	0	0	1	0	0	0	1	0
2	0	0	0	0	1	1	1	2	2	2	1	2	2	2	1
0	2	2	0	1	2	0	1	2	0	1	2	2	0	1	2
0	0	1	0	2	2	1	1	2	1	1	2	2	1	1	2

Бу ерда ҳам юқорида баён этилган усулда КРОМ хизматларидан фойдаланиш имконияти мавжудлиги шубҳага ўрин қолдирмайди.

6.6 Электрон рақамли имзо криптотизимини яратишга RSA усулида ёндашув

Юқорида кўриб ўтилган RSA усулида ёндашув асосида криптотизим яратишда, агар шифрловчи томон ўз модули ва махфий калитидан фойдаланса, шифр очувчи томон фақатгина

шифрловчи томоннинг ошкора калитидан фойдаланади деб ҳисобланса, у ҳолда шифрловчи томоннинг жўнатмаси ЭРИ бўлиб, шифр очувчи томон эса шифрловчи томоннинг электрон рақамли имзоси билан тасдиқланган дастлабки матнга эга бўлади. Бу ерда d — шифрнинг махфий калити, e — шифрнинг ошкора калити деб белгилаш кифоя. Шифр ва электрон рақамли имзо криптотизимининг тармоқдаги ҳар бир фойдаланувчиси ўз модулларига ва ошкора-махфий калитлар жуфтлигига эга бўлиши зарур. Чунки, бегоналар учун махфий ахборот жўнатишда ахборот ҳам шифрланган, ҳам имзоланган бўлиши зарур. Қуйида шундай криптотизимлар яратишга ёндашув ҳақида сўз боради.

Криптотизимда куйидаги параметрлар фойдаланилади:

a) n_t — модуль, бу ерда $n_t = p_{1t} * p_{2t}$; p_{1t}, p_{2t} — ҳар хил махфий туб сонлар, $t \in \{1,2... k\}$, k — тармоқ тугунлари сони, p_{1t}, $p_{2t} > 2^{255}$. Туб сонларнинг юқори чегараси криптотизим муайян амалга оширилганда белгиланиши керак;

b) (e_t, d_t) — n_t нинг Эйлер пи-функцияси $\varphi(n_t)$ киймати бўйича ўзаро тескари бутун сонлар жуфтлиги, e_t — шифрнинг ошкора калити d_t — шифрнинг махфий калити, бу ерда $1 < e_t, d_t < \varphi(n_t)$;

R, r_1, r_2 — шифрлаш ва шифр очиш учун ошкора ёки махфий параметрлар, бу ерда $1 \leq R$, r_1, $r_2 < n_t$; параметр R фақат тармоқда қонуний фойдаланувчилар учунгина маълум бўлиб, уни томонларга тарқатиш протоколга мувофиқ амалга оширилади. r_1, r_2 параметрлар камида бешта маромда ҳосил қилиниши мумкин:

1-маромда дастлабки матннинг биринчи блокини шифрлаш учун параметр сифатида дастлабки матннинг хэш-функцияси киймати r ни R га кўпайтмасидан фойдаланилади. $i>1$ учун дастлабки матннинг $i+1$- блок шифрматнини $i+1$- блок, i-блок шифрматни ва i-блокнинг модуль бўйича тескари қийматига кўпайтмаси шаклида ҳосил қилинади. Шифрматн блоклари билан бирга хэш-функция киймати r параметр R имзоланиб жўнатилади. Қабул қилувчи томонда қўшимча шифрматн r' га ўгирилгач, шифрматн биринчи блоки дастлабки матнга

ўгирилади ва кўпайтириш ҳамда тескарилаш амалларидан фойдаланиб дастлабки матннинг қолган блоклари тикланади. *r'* дастлабки матн хэш-функцияси қиймати билан таққосланади;

2-маромда дастлабки матн (шифрматн)нинг ҳар бир блокини шифрлаш учун, параметр сифатида, дастлабки матннинг хэш-функцияси қиймати *r* нинг *R* га кўпайтмасидан фойдаланилади. *r* шифрматн билан бирга параметр *R* бўйича қўшимча шифрматнга ўгириб жўнатилади. Қабул қилувчи томон қўшимча шифрматнни *r'* га ўгириб, асосий шифрматнни дастлабки матнга ўгиради ва *r'* дастлабки матн хэш-функцияси қиймати билан таққосланади;

3-маромда шифрлаш ва дастлабки матнга ўгириш параметрлари бир-бирига тенг бўлиб, тасодифий сон *r* сифатида генерацияланади ва махфий сакланади. Параметр *r* ни томонларга таркатиш протоколига биноан амалга оширилади;

4-маромда дастлабки матн (шифрматн) биринчи блокини шифрлаш учун параметр сифатида *R* дан, кейинги блокларни шифрлаш учун ундан аввалги блокларнинг шифрлаш натижалари бўлган сонлардан фойдаланилади. Бундай маром симметрик шифрлардаги блокларни илактириш маромига ўхшашдир;

5-маромда дастлабки матн (шифрматн) тоқ блокларини шифрлаш учун параметр сифатида унинг жуфт блоклари кийматининг параметр *R* га кўпайтмасидан фойдаланилади. Жуфт блоклар параметр *R* билан шифрматн (дастлабки матн) га ўгирилади.

Дастлабки матн блокларини шифрматн блокларига, шифрматн блокларини дастлабки матн блокларига алмаштириш юқоридаги маромларга мос тарзда қуйидаги ифодалар асосида бажарилади:

1-маром.

t-томонда ЭРИ шакллантиришда

$r_1 = h(M)$ ҳисобланади.

$i = 1$ учун, $r = R * r_1$ параметрли

$SM_1 \equiv M_1^{\backslash\backslash\, dt} \pmod{n_t}$ ҳисобланади.

$i \in \{2, \ldots b\}$ учун

$SM_i \equiv M_i * SM_i * M_1^{-1} \ (mod\ n_t)$ ҳисобланади.

$r = R$ параметрли

$Sr \equiv r^{|dt} \ (mod\ n_t)$ ҳисобланади.

Sr, SM_1, SM_2,.... SM_{b-1}, SM_b қабул қилувчи 2-томонга жўнатилади.

2-томонда ЭРИ ҳақиқийлигини тасдиқлашда

$r = R$ параметрли

$r' \equiv Sr^{|et} \ (mod\ n_t)$ ҳисобланади.

$i = 1$ учун, $r = R * r'$ параметрли

$M_1 \equiv SM_1^{\backslash\backslash\backslash et} \ (mod\ n_t)$ ҳисобланади.

$i \in \{2, \ldots b\}$ учун

$M_i \equiv SM_i * M_1 * SM_1^{-1} \ (mod\ n_t)$ ҳисобланади.

$r_2 = h(M)$ ҳисобланади.

6.7-мисол

t-томонда ЭРИ шакллантириш

n_t	p_t	q_t	$\varphi(n_t)$	d_t	R	M_1	M_2	M_3	M_4	$r_1 = h(M)$	$r = R * r_1$
221	17	13	192	119	75	28	54	71	81	101	61

Sr_1	SM_1	SM_2	SM_3	SM_4
129	199	147	181	110

2-томонда ЭРИ ҳақиқийлигини тасдиқлаш

n_t	e_t	R	r'	$r = R * r'$	M_1	M_2	M_3	M_4	$r_2 = h(M)$
221	71	75	101	61	28	54	71	81	101

Агар $r_2 = r'$ бўлса, жўнатилган ахборот ҳамда ЭРИ ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади.

2-маром.

t-томонда ЭРИ шакллантиришда

$r_1 = h(M)$ ҳисобланади.

$i \in \{1, 2, \ldots b\}$ учун, $r = R * r_1$ параметрли

$SM_i \equiv M_i^{\backslash\backslash dt} \pmod{n_t}$ ва

$r = R$ параметрли

$Sr \equiv r_1^{|dt} \pmod{n_t}$ ҳисобланади ва

Sr, SM_1, SM_2,.... SM_{b-1}, SM_b қабул қилувчи 2-томонга жўнатилади.

2-томонда ЭРИ ҳақиқийлигини тасдиқлашда

$r = R$ параметрли

$r_1 \equiv Sr^{|et} \pmod{n_t}$ ҳисобланади.

$i \in \{1,2,... b\}$ учун, $r = R * r_1$ параметрли

$M_i \equiv SM_i^{\backslash\backslash et} \pmod{n_t}$ ҳисобланади.

$r_2 = h(M)$ ҳисобланади.

Агар $r_2 = r_1$ бўлса, жўнатилган ахборот ҳамда ЭРИ ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади.

3-маром.

t-томонда ЭРИ шакллантиришда

$i \in \{1,2,... b\}$ учун, $r = r_{t2}$ параметрли

$SM_i \equiv M_i^{|dt} \pmod{n_t}$ ҳисобланади ва

SM_1, SM_2,.... SM_{b-1}, SM_b қабул қилувчи 2-томонга жўнатилади.

2-томонда ЭРИ ҳақиқийлигини тасдиқлашда

$i \in \{1,2,... b\}$ учун, $r = r_{t2}$ параметрли

$M_i \equiv SM_i^{|et} \pmod{n_t}$ ҳисобланади.

Агар дастлабки матн мазмунга ва келишилган форматга эга бўлса, жўнатилган ахборот ҳамда ЭРИ ҳақиқий, акс ҳолда ноҳақиқий деб топилади;

Бу ерда $^|$ — параметр $r = r_{t2}$ билан дискрет даражага ошириш рамзи.

4-маром.

t томонда ЭРИ шакллантиришда

$i = 1$ учун, $r = R$ параметрли

$SM_1 \equiv M_1^{| dt} \pmod{n_t}$ ҳисобланади.

$i \in \{2,... b\}$ учун, $r = SM_{i-1}$ параметрли

$SM_i \equiv M_i^{\backslash\backslash dt} \pmod{n_t}$ ҳисобланади ва

SM_1, SM_2.... SM_{b-1}, SM_b қабул қилувчи 2-томонга жўнатилади.

2-томонда ЭРИ ҳақиқийлигини тасдиқлашда

$i=1$ учун, $r=R$ параметрли

$M_1 \equiv SM_1^{|et} \ (mod\ n_t)$ ҳисобланади.

$i \in \{2, ... b\}$ учун, $r=M_{i-1}$ параметрли

$M_i \equiv SM_i^{\backslash\backslash et} \ (mod\ n_t)$ ҳисобланади.

Агар дастлабки матн мазмунга ва келишилган форматга эга бўлса, жўнатилган ахборот ҳамда ЭРИ ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади.

5-маром.

t томонда ЭРИ шақллантиришда

$i \in \{1,3,,... b-1\}$ учун, $r=R * M_{i+1}$ параметрли

$SM_i \equiv M_i^{\backslash\backslash dt} \ (mod\ n_t)$ ҳисобланади.

$i \in \{2,4,,... b\}$ учун, $r=R$ параметрли

$SM_i \equiv M_i^{|dt} \ (mod\ n_t)$ ҳисобланади ва

SM_1, SM_2.... SM_{b-1}, SM_b қабул килувчи 2-томонга жўнатилади.

2-томонда ЭРИ ҳақиқийлигини тасдиқлашда

$i \in \{2,4,,... b\}$ учун, $r=R$ параметрли

$SM_i \equiv M_i^{|et} \ (mod\ n_t)$ ҳисобланади.

$i \in \{1,3,,... b-1\}$ учун, $r=R * M_{i+1}$ параметрли

$SM_i \equiv M_i^{\backslash\backslash et} \ (mod\ n_t)$ ҳисобланади.

Агар дастлабки матн мазмунга ва келишилган форматга эга бўлса, жўнатилган ахборот ҳамда ЭРИ ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади.

Келтирилган маромлар RSA криптотизимига оид шифрлашнинг коммутативлиги билан алоқадор камчиликларни бартараф этишга имкон беради ва ўзининг RSA криптотизими билан тенг криптобардошлилиги ҳамда қонуний фойдаланувчи бўлмаганлар учун RSA криптотизимига нисбатан юқори криптобардошлилиги билан тавсифланади.

6.7 Электрон рақамли имзо криптотизимини яратишга умумий схема усулида ёндашув

6.7.1 Даража параметри муаммосининг мураккаблигига асосланган ЭРИ умумий схемаси

Криптобардошлилиги даража параметри муаммосининг мураккаблигига асосланган ЭРИ криптотизимларини яратишга ҳам 1-бўлимда келтирилган умумий схема [1] усулида ёндашув мақсадга мувофиқдир.

1-бўлимда келтирилган схемаларнинг заиф томони шундаки, бадният криптотаҳлилчи дискрет логарифм муаммосини ҳал қилиш учун етарли ресурсларга эга бўлиб, уни сохталаштирган бўлса, унда сохта ЭРИ ҳам ҳақиқий деб қабул килинади. Натижада қонуний ҳуқуққа эга фойдаланувчи томонларнинг ЭРИ сохталигини исботлаш имкониятлари йўққа чиқади. Бунинг олдини олиш йўлларидан бири ошкора калит ифодасида даража асоси a ни махфий параметрлар гуруҳига ўтказиб, ошкора калитлар сонини биттага орттиришдир ҳамда параметрли функциядан фойдаланишдир. Бунда ЭРИ криптотизимининг бардошлилиги, даража параметри муаммосининг мураккаблигига асосланган, криптотизим бардошлилиги билан белгиланади. Бу ҳол қуйида ҳисобга олинган.

Даража параметри муаммосининг таърифида қатнашган ифода $y \equiv g^{\backslash x} (mod\ p)$ да g чекли тўплам $GF(p)$ нинг параметр R билан ҳосил қилувчи (генератор) элементи сифатида белгиланган.

Даража параметри муаммосининг мураккаблигига асосланган ЭРИ криптотизимини яратишда, ЭРИ биринчи ошкора калити $y \equiv g^{\backslash x} (mod\ p)$ шаклини олади. Унда ЭРИ иккинчи ошкора калити $z \equiv g^{\backslash u} (mod\ p)$ шаклида генерацияланади. Бу ерда g — махфий асос, x, u — махфий даража кўрсаткичларидир, $\backslash$ — параметр R билан дискрет даражага ошириш рамзи; махфий асос g ва параметр R нинг 1 билан p оралиғида танланади; асос g параметр R билан даражага оширилганда фақатгина даража кўрсаткичи q бўлгандагина 0 га тенг бўлиш шартини

қаноатлантирувчи натурал сондир; бу ерда $q = p - 1$ ёки $(p - 1)$ нинг катта туб кўпайтувчиси — факторидир.

Икки ошкора калитли ЭРИ ҳам икки қисмдан иборат бўлиб, унинг биринчи қисми $r \equiv g^{k} \pmod{p}$ шаклида, иккинчи қисми s қуйидаги умумлашган ифода асосида ҳисобланади:

$$a * k \equiv b * u + c * x \pmod{q},$$

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{a} \equiv z^{b} \cdot y^{c} \pmod{p},$$

шаклини олади. Бу ерда ҳам a, b, c параметрларининг ўрнига [23] да келтирилган r', s, M лардан иборат тўпламда аниқланган унар ва бинар амал натижаларидан тузилган жадвал бўйича ўрнига қўйишлардан фойдаланилганда даража параметри муаммосининг мураккаблигига асосланган 120 хил ЭРИ схемаси келиб чиқади; бу ерда $r' \equiv r \pmod{q}$, M — дастлабки матн.

Масалан, агар $a \leftarrow r'$, $b \leftarrow s$, $c \leftarrow M$ ўрнига қўйишдан фойдаланилса, иккинчи қисм s учун умумлашган ифода

$$r' * k \equiv s * u + M * x \pmod{q}$$ шаклини,

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{r'} \equiv z^{s} \cdot y^{M} \pmod{p}$$ шаклини олади.

Агар $a \leftarrow r'$, $b \leftarrow M$, $c \leftarrow s$ ўрнига қўйишдан фойдаланилса, иккинчи қисм s учун умумлашган ифода

$$r' * k \equiv M * u + s * x \pmod{q}$$ шаклини,

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{r'} \equiv z^{M} \cdot y^{s} \pmod{p}$$ шаклини олади.

Агар $a \leftarrow r' * M$, $b \leftarrow s$, $c \leftarrow 1$ ўрнига қўйишдан фойдаланилса, иккинчи қисм s учун умумлашган ифода

$$r' * M * k \equiv s * u + x \pmod{q}$$ шаклини,

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{r' * M} \equiv z^{s} \cdot y \pmod{p}$$ шаклини олади.

Агар $a \leftarrow s$, $b \leftarrow r' * M$, $c \leftarrow 1$ ўрнига қўйишдан фойдаланилса, иккинчи қисм s учун умумлашган ифода

$$s * k \equiv r' * M * u + x \pmod{q}$$ шаклини,

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{s} \equiv z^{r' * M} \cdot y \pmod{p}$$ шаклини олади.

Шунингдек, агар $a \leftarrow s$, $b \leftarrow M$, $c \leftarrow r'$ ўрнига қўйишдан фойдаланилса, DSA [93] ва ГОСТ Р 34.10-94 [91] юзага келиши учун асос бўлган Тоҳир Ал Жамол усулига мос икки ошкора калитли ва махфий асосга эга ЭРИ схемаси келиб чиқади. Бунда иккинчи қисм s учун умумлашган ифода

$$s * k \equiv M * u + r' * x \ (mod\ q)$$ шаклини,

ЭРИ ҳақиқийлигини тасдиқлаш таққосламаси эса

$$r^{\backslash s} \equiv z^{\backslash M} \ ® \ y^{\backslash r} \ (mod\ p)$$ шаклини олади.

Келтирилган ифодаларда $\backslash$ — параметр R билан дискрет даражага ошириш рамзи бўлиб, ЭРИ нинг биринчи қисмини, иккала ошкора қалитларни ҳисоблаб топишда ва ЭРИ ҳақиқийлигини тасдиқлаш таққосламасини ҳисоблашда параметр R бир хил қийматга эгадир. Бундай ҳол ЭРИ дан фойдаланишнинг биргина маромидир холос. ЭРИ дан камида 3 хил маромда фойдаланиш мумкин:

a) 1-маромда параметр $R>1$ бўлиб, у ЭРИ нинг биринчи қисмини, иккала ошкора калитларни ҳисоблашда ва ЭРИ ҳақиқийлигини тасдиқлаш таққосламасини хисоблашда бир хил қийматга эга;

b) 2-маромда иккала ошкора калитни ҳисоблашда параметр $R=1$, ЭРИ нинг биринчи қисмини ва ЭРИ ҳақиқийлигини тасдиқлаш таққосламасини ҳисоблашда параметр $R>1$ бир хил қийматга эга;

c) 3-маромда иккала ошкора калитларни ҳисоблашда параметр $R>1$, ЭРИ нинг биринчи қисмини ва ЭРИ ҳақиқийлигини тасдиқлаш таққосламасини ҳисоблашда параметр $R_1>1$ бошқа қийматга эга.

Агар параметрдан уч хил маромда фойдаланиш мумкинлиги ҳисобга олинса, унда даража параметри муаммосининг мураккаблигига асосланган ЭРИ схемалари сони икки марта кўпайиб, *360* тага етади. Юқорида эслатиб ўтилган эквивалент шакллар ва бошқа ўзгартиришлар натижасида ЭРИ схемаларининг сони *39000* дан ортиб кетади. Агар ЭРИ схемаларида дискрет логарифм муаммосини ечиш орқали ЭРИ сохталаштирилган бўлса, уни аниқлаш имконини берадиган кейинги бандда назарда тутилган усулдан фойдаланиш имкониятини

ҳам ҳисобга олинса, ЭРИ схемаларининг сони *78000* дан ортиб кетади.

Схемалар орасида RSA ЭРИ схемаси каби, ЭРИ ҳақиқийлигини тасдиқлаш жараёнида дастлабки матн *M* ёки унинг хэш-қиймати *m* ҳосил бўладиган *p*-NEW [23, 25] схемасининг ўрнига, даража параметри муаммосининг мураккаблигига асосланган ЭРИ нинг қуйидаги схемасини ҳосил қиламиз:

1-маром:

ошкора калитлар

$y \equiv g^{\backslash\backslash x} \ (mod\ p)$,

$z \equiv g^{\backslash\backslash u} \ (mod\ p)$.

ЭРИ шакллантириш

$r \equiv m$ ®' $g^{\backslash\backslash -k} \ (mod\ p)$,

$s \equiv u^{-1} * (\ k - r' * x) \ (mod\ q)$.

ЭРИ ҳақиқийлигини тасдиқлашда

$m \equiv z^{\backslash\backslash s}$ ®' $y^{\backslash\backslash\ r'}$ ®' $r \ (mod\ p)$

дастлабки матн ёки унинг хэш-қиймати ҳосил бўлади.

6.8-мисол:

ЭРИ шакллантириш

m	*p*	*q*	*g*	*x*	*u*	u^{-1}	*R*	R^{-1}	*k*	$g^{\backslash -k}$	$r = r'$	*s*
30	*107*	*53*	*8*	*19*	*17*	*25*	*31*	*38*	*7*	*40*	*34*	*31*

ЭРИ ҳақиқийлигини тасдиқлаш

p	*q*	*y*	*z*	*R*	*R-1*	$r = r'$	*s*	$z^{\backslash s}$	$y^{\backslash r}$	*m*
107	*53*	*28*	*57*	*31*	*38*	*34*	*31*	*21*	*50*	*30*

2-маром:

ошкора калитлар

$y \equiv g^{\backslash x} \ (mod\ p)$,

$z \equiv g^{\backslash u} \ (mod\ p)$.

ЭРИ шакллантириш

$r \equiv m$ ®' $(R^{-1} * g)^{\backslash\backslash -k} \ (mod\ p)$,

$s \equiv u^{-1} * (\ k - r' * x) \ (mod\ q)$.

ЭРИ ҳақиқийлигини тасдиқлашда
$m \equiv (R^{-1} * z)^{\backslash\backslash s}$ ®' $(R^{-1} * y)^{\backslash\backslash r'}$ ®' $r \pmod p$
дастлабки матн ёки унинг хэш-қиймати ҳосил бўлади.
6.9-мисол:

ЭРИ шакллантириш

m	p	q	g	x	u	u^{-1}	R	R^{-1}	k	$(R^{-1} * g)^{\backslash\backslash -k}$	$r = r'$	s
29	107	53	8	19	17	25	31	38	7	68	25	13

ЭРИ ҳақиқийлигини тасдиқлаш

p	q	y	z	$r = r'$	s	R	R^{-1}	$(R^{-1} * z)^{\backslash\backslash s}$	$(R^{-1} * y)^{\backslash\backslash r'}$	m
107	53	60	9	25	13	31	38	56	84	29

3-маром:
ошкора калитлар
$y \equiv g^{\backslash\backslash x} \pmod p$,
$z \equiv g^{\backslash\backslash u} \pmod p$.
ЭРИ шакллантириш
$r \equiv m$ ®" $(R_1^{-1} * R * g)^{\backslash\backslash -k} \pmod p$,
$s \equiv u^{-1} * (k - r' * x) \pmod q$.
ЭРИ ҳақиқийлигини тасдиқлашда
$m \equiv (R_1^{-1} * R * z)^{\backslash\backslash s}$ ®"$(R_1^{-1} * R * y)^{\backslash\backslash r'}$ ®"$r \pmod p$.
6.10-мисол:

ЭРИ шакллантириш

m	p	q	g	x	u	u^{-1}	R	R^{-1}	R_1	R_1^{-1}	k	$g^{\backslash -k}$	$r = r'$	s
30	107	53	8	19	17	25	31	38	47	41	7	15	9	34

ЭРИ ҳақиқийлигини тасдиқлаш

p	q	y	z	R	R^{-1}	R_1	R_1^{-1}	$r = r'$	s	$z^{\backslash s}$	$y^{\backslash r}$	m
107	53	28	57	31	38	47	41	9	34	79	45	30

дастлабки матн ёки унинг хэш-қиймати ҳосил бўлади.

Бу ерда махфий асос g нинг 1 билан q оралиғида 1-, 2-маромларда параметр $R>1$ билан, 2-маромда параметр $R=1$ билан, даражага оширилганда фақатгина даража кўрсаткичи q бўлгандагина 0 га тенг бўлиши мумкин бўлган натурал сон;

$q = p - 1$ ёки $(p - 1)$ нинг катта туб кўпайтувчиси — факторидир;

x, u — махфий даража кўрсаткичлари, $'$ — параметр $R=1$ билан дискрет даражага ошириш рамзи, $''$ — параметр $R>1$ билан дискрет даражага ошириш рамзи, $'''$ — параметр $R_1>1$ билан дискрет даражага ошириш рамзи, ® — параметр $R=1$ билан кўпайтириш рамзи, ®' — параметр $R>1$ билан кўпайтириш рамзи, ®'' — параметр $R_1>1$ билан кўпайтириш рамзи.

Шуни таъкидлаш жоизки, ЭРИ нинг иккинчи қисми келтирилган ифодаларда иштирок этган махфий даража кўрсаткичи $u^1 \equiv u \pmod q$ фақат дастлабки сеансдагина ҳисобланиб, навбатдаги сеансларда фойдаланиш учун махфий хотирада u ўрнига ёзиб қўйилади. Шунинг учун u нинг тескариланиши ЭРИни шакллантириш жараёнига салбий таъсир кўрсатмайди.

6.7.2 ЭРИнинг сохта ёки ҳақиқийлигини аниқлаш

ЭРИ умумий схемаларидан конуний фойдаланувчи томон аслида нияти бузуқ бўлиб, дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлса, у ЭРИни сохталаштириши мумкин. Ноқонуний фойдаланувчи томонларнинг бунга имкониятлари бўлиши эҳтимоллиги нолга якин, чунки улардан махфий параметрлар сир тутилади.

Бадният қонуний фойдаланувчи дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлганда ҳам ЭРИни сохталаштириш учун махфий даража асоси g ўрнига сохта асос g' дан фойдаланишга мажбур, чунки ҳақиқий a унга номаълум.

Бадният қонуний фойдаланувчи шу йўсинда ЭРИни сохталаштириш имконига эга деб ҳисобланган ҳолда, ЭРИ сохталигини аниқлаш калитидан фойдаланишга асосланган назорат сеанс калити усули (НСКУ) [100] да баён этилган. Унда элек-

трон рақамли имзо бўйича давлат стандарти O‘z DSt 1092:2005 га хос НСКУ га асосланган протоколлардан фойдаланилганда, ЭРИ сохталигини аниқлаш имконияти мавжудлиги исботланган. Шуни эътиборга олиб, ЭРИ сохталигини аниқлаш масалаларига ортикча тўхталиб ўтирмаймиз.

6.7.3 Даража параметри муаммосининг мураккаблигига асосланган ЭРИ алгоритми

Криптобардошлилиги даража параметри муаммосининг мураккаблигига асосланган ЭРИ схемалари тўпламининг ҳар биридан фойдаланувчи аввало ЭРИ дан фойдаланиш маромини танлаши лозим. 1-маромда параметр $R>1$ фойдаланувчилар гуруҳи учун ўзаро махфий бўлса, 2-маромда параметр $R>1$ фойдаланувчилар жуфти учун ўзаро махфий, 3-маромда параметр $R>1$ фойдаланувчилар гуруҳи учун ўзаро махфий бўлиб, $R_1>1$ фойдаланувчилар жуфти учун ўзаро махфий ҳисобланиб, гуруҳнинг бошқа аъзоларидан сир тутилади.

Ҳар учала маромда ҳам фойдаланувчиларнинг параметрлари тўплами қуйидагиларни ўз ичига олади:

a) p — модуль, туб сон, бу ерда $p > 2^{255}$. Бу соннинг юқори чегараси электрон рақамли имзо алгоритми муайян амалга оширилганда аниқланиши керак;

b) q — $(p-1)$ нинг фактори (туб кўпайтувчиси) бўлган туб сон, бу ерда $2^{254}<q<2^{256}$;

c) $m = H(\bullet)$ — хэш-функция, чекланган узунликдаги M хабарни 256 бит узунликдаги иккилик векторида акс эттиради;

d) *1-маром учун* R — ягона параметрдан, 2-маром учун параметрлар жуфти $(1, R)$ дан, 3-маром учун параметрлар жуфтидан фойдаланилади. R, R_1, бу ерда $1<R$, $R_1 < p$ шартни қаноатлантирувчи натурал сонлар.

Ҳар бир фойдаланувчи қуйидаги шахсий калитларга эга бўлиши керак:

a) (x, u, g) — бутун сонлар учлиги — ЭРИнинг махфий калити;

бу ерда: x, u — махфий калитлар, $1 < x, u < q$ шартларни қаноатлантирувчи тасодифий ёки псевдотасодифий генерацияланган бутун тоқ сонлар;

g — махфий калит, $g \equiv h^{\backslash(p-1)/q} \pmod p$ 1-, 3-маромларда параметр $R > 1$ билан, 2-маромда $R = 1$ билан ҳисобланадиган натурал сон;

бу ерда: $h < p$ — махфий натурал сон бўлиб, ω нинг $1 \div (p-1)/q$ оралиқ қийматларида фақат $\omega = (p-1)/q$ бўлгандагина $g^{\backslash\omega} (mod p) \equiv 0$ шартни каноатлантиради;

b) (y, z) — бутун сонлар жуфтлиги — ЭРИнинг ошкора калити;

бу ерда: y, z — ошкора калитлар икки хил ифодалар ёрдамида ҳисобланади:

1-, 3-маромлар учун: $y \equiv g^{\backslash\backslash x} \pmod p$, $z \equiv g^{\backslash\backslash u} \pmod p$;

2-маром учун: $y \equiv g^{\backslash x} \pmod p$, $z \equiv g^{\backslash u} \pmod p$;

бу ерда x, u — махфий даража кўрсаткичлари, $^{\backslash}$— параметр $R=1$ билан дискрет даражага ошириш рамзи, $^{\backslash\backslash}$— параметр $R>1$ билан дискрет даражага ошириш рамзи.

Фойдаланувчилар гуруҳи учун p, q туб сонлари ошкора ва умумий бўлиши мумкин.

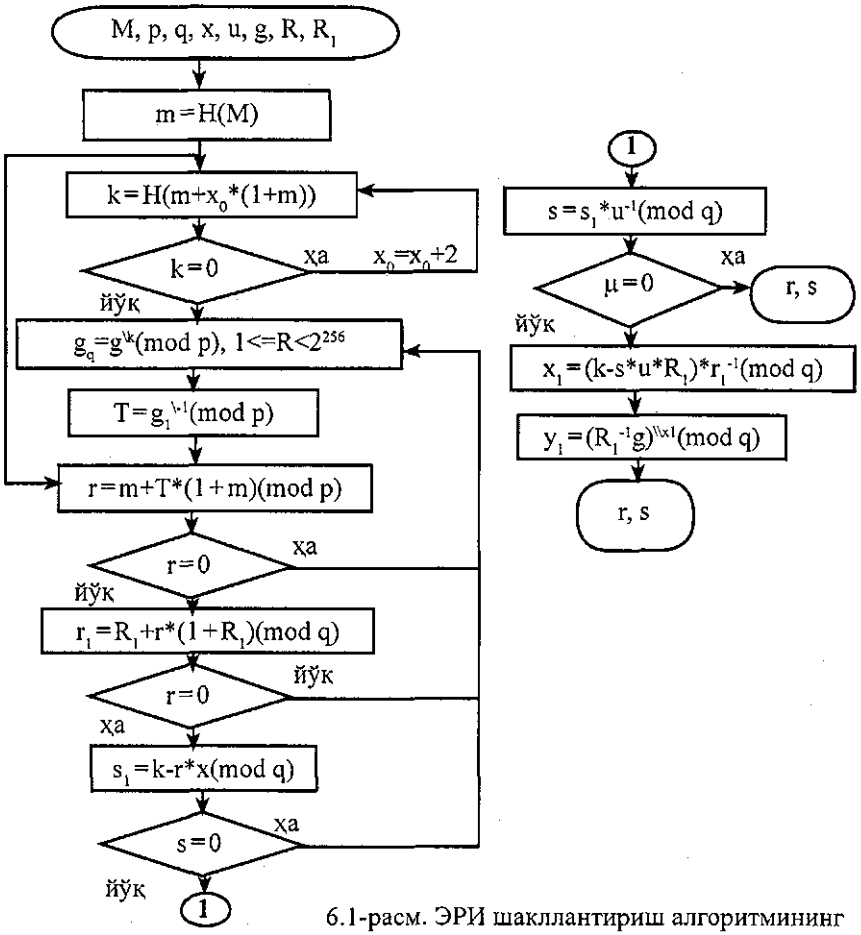
Электрон рақамли имзони шакллантириш ва ЭРИ ҳакикийлигини тасдиклаш алгоритмлар асосида амалга оширилади. Электрон рақамли имзо ва сеанс калитини шакллантириш жараёни тугагач, имзоланган хабар (ҳабар ва тўлдирувчи) қабул қилувчи томонга узатилади. Қабул қилувчи ва\ёки назорат килувчи томонга ЭРИ сохталигини аниқлаш калити — сеанс калити ҳам узатилади. Бунда, ошкора параметрлар ва биргаликдаги махфий калит параметри R гуруҳ аъзоларга етказилган деб ҳисобланади.

6.1-, 6.2-расмларда давлат стандарти O‘z DSt 1092:2005 учун ЭРИ ва сеанс калитини шакллантириш ҳамда ЭРИ ҳақиқийлигини тасдиқлаш алгоритмларининг структура схемалари келтирилган.

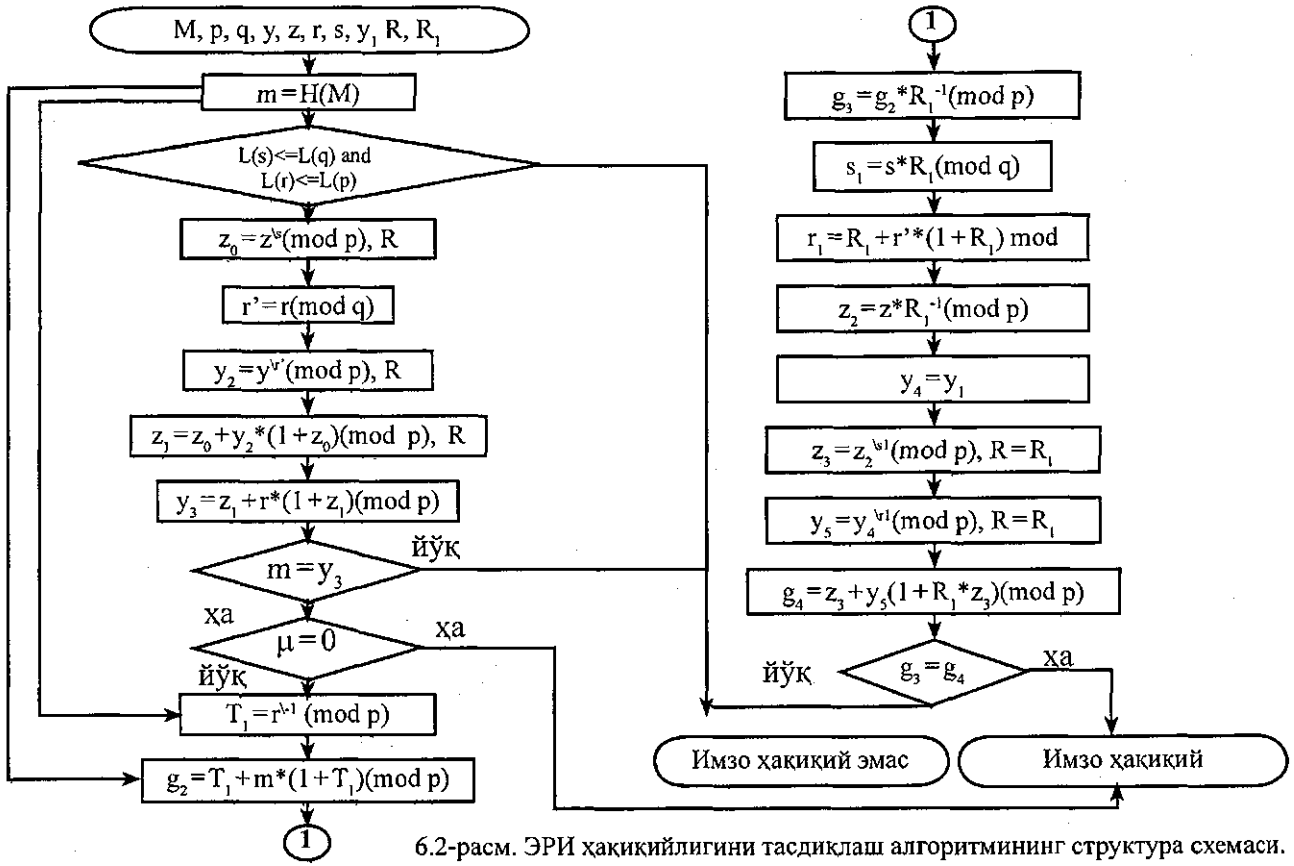
ЭРИ ва сеанс калитини шакллантириш жараёни учун дастлабки (киришдаги) маълумотлар бўлиб хабар M, ЭРИнинг махфий калити (x, u, g), параметр R, назорат калити R_p, модуль p ва

q сони ҳисобланади. Чиқиш натижаси бўлиб ЭРИ (s, r) ва сеанс калити y_1 ҳисобланади.

ЭРИ ҳақиқийлигини тасдиқлаш жараёни учун дастлабки (киришдаги) маълумотлар бўлиб имзоланган M хабар, электрон рақамли имзо s, r, ошкора калитлар y, z, параметр R, назорат калити R_1, модуль p ва q сони, чиқиш натижаси бўлиб эса мазкур ЭРИнинг ҳақиқийлиги ёки ҳақиқий эмаслиги ҳақидаги ахборот ҳисобланади.



6.1-расм. ЭРИ шакллантириш алгоритмининг структура схемаси.



6.2-расм. ЭРИ ҳақиқийлигини тасдиқлаш алгоритмининг структура схемаси.

6.8 RSA шифрлаш ва Диффи-Хэллман калит алмашиш алгоритмларини параметрли алгебра асосида ишлаб чиқилган алгоритмлар билан гармонизациялаш

Маълумки, RSA шифрлаш ва Диффи-Хэллман калит алмашиш алгоритмлари дунёда жуда кенг қўлланилади. Шунинг учун ушбу алгоритмларни параметрлар алгебраси асосида ишлаб чиқилган алгоритмлар билан гармонизациялаш масаласини ҳал қилиш, янги тизимларнинг мавжуд тизимлар билан ҳам ишлай олиш имконини беради.

RSA шифрлаш алгоритми

Фараз қилайлик, *j*-томон параметрли алгебра асосида такомиллаштирилган RSA шифрлаш алгоритми асосида ишлайдиган тизимга, *i*-томон эса мавжуд RSA шифрлаш алгоритми асосида ишлайдиган тизимга эга. Матнни шифрлаш учун у *i*-томоннинг эълон қилган ошкора калити e_i ёрдамида қуйидаги амалларни бажаради:

j-томонда

$M = M_1, M_2, \ldots M_b$, $i \in \{1,2,\ldots b\}$ учун,

$SM_i \equiv (M_i - 1)^{\backslash e_i} + 1 \pmod{n_i}$ ҳисобланади ва $SM_1, SM_2, \ldots SM_{b-1}, SM_b$ қабул қилувчи *i*—томон (махфий ва ошкора калитлар эгаси)га жўнатилади. Бу ерда $^{\backslash e_i}$ параметр $R = 1$ бўйича e_i — даражага ошириш рамзи.

i-томонда шифрматнни дастлабки матнга ўгиришда

$i \in \{1,2,\ldots b\}$ учун, $M_i \equiv SM_i^{\backslash d_i} \pmod{n_i}$ ҳисоблайди.

6.11-мисол:

j-томонда шифрматн шакллантириш

n_i	e_i	R	M_0	M_1	M_2	M_3	SM_0	SM_1	SM_2	SM_3
299	71	1	25	26	27	28	275	13	60	64

i-томонда шифрматнни дастлабки матнга ўгириш

n_i	p_i	q_i	$\varphi(n_i)$	d_i	SM_0	SM_1	SM_2	SM_3	M_0	M_1	M_2	M_3
299	13	23	264	119	275	13	60	64	25	26	27	28

Диффи-Хэллман калит алмашиш алгоритми

Фараз қилайлик, *j*-томон параметрли алгебра асосида такомиллаштирилган Диффи-Хэллман калит алмашиш алгоритми асосида ишлайдиган тизимга, *i*-томон эса мавжуд Диффи-Хэллман калит алмашиш алгоритми асосида ишлайдиган тизимга эга.

Махфий калит алмашиш жараёни (p, a) жуфтлик маълум саналиб, қуйидаги қадамларни ўз ичига олади:

1-қадам: *i*-томон, ўз махфий калити e_i ни тасодифий сон сифатида танлаб, ўз ошкора калити

$y_i \equiv a^{e_i} (mod\ p)$ ни ҳисоблайди ва уни умумий маълумотлар базасига ёки *j*-томонга жўнатади;

2-қадам: *j*-томон, ўз махфий калити d_j ни тасодифий сон сифатида танлаб, ўз ошкора калити

$y_j \equiv (a\text{-}1)^{\backslash d_j} + 1 (mod\ p)$ ни ҳисоблайди ва уни умумий маълумотлар базасига ёки *i* -томонга жўнатади. Бу ерда параметр $R=1$;

3-қадам: *j*-томон *i*-томоннинг ошкора калитини қабул қилиб,

$k_j \equiv (y_i\text{-}1)^{\backslash d_j} + 1 (mod\ p)$ ни ҳисоблайди;

4-қадам: *i*-томон *j*-томоннинг ошкора калитини қабул қилиб,

$k_i \equiv y_j^{e_i} (mod\ p)$ ни ҳисоблайди, бу ерда *i*-, *j*-томонларнинг умумий махфий калити $k = k_i = k_j$.

6.12-мисол:

p	a	R	e_i	d_j	y_i	y_j	k_j	k_i
17	5	1	11	13	11	3	7	7

Модуль p фойдаланувчилар гуруҳи учун умумий, асос a эса фойдаланувчилар гуруҳи учун бир хил ёки фойдаланувчилар жуфтлари учун ҳар хил бўлиши мумкин.

Параметр $R=1$ бўлганда, худди шундай услубда бошқа ишлаб чиқилган алгоритмларни ҳам мавжуд алгоритмлар билан гармонизациялаш мумкин.

Бунда жорий криптотизимларнинг бардошлилиги иккала томон учун ҳам, бошқа томонлар учун ҳам бир хил бўлади. Агар параметр $R>>1$ олинса ва бу параметр ёпиқ калит вазифасини бажарса, унда жорий криптотизимларнинг бардошлилигини оширишга эришилади.

6.9 Электрон ҳужжат алмашиш тизими "Е-ҲУЖЖАТ"

Юқорида келтирилган маълумотларни шифрлаш, электрон рақамли имзо ва махфий калитларни алмашиш алгоритмлари асосида, муаллиф раҳбарлигида IntSoft Servis корхонаси ходимлари билан ҳамкорликда, Е-ҲУЖЖАТ ва Е-ХАТ электрон ҳужжат ва хат алмашиш тизимлари ҳамда Электрон рақамли имзо қалитларини рўйхатга олиш маркази дастурий таъминоти ва турли тизимлар учун ҳимоя воситаси — криптопровайдер ишлаб чиқилди.

Е-ҲУЖЖАТ давлат ва тижорат корхоналарида электрон ҳужжат алмашиш тизимини юритиш учун мўлжалланган.

Е-ҲУЖЖАТ мамлакатимизда ишлаб чиқилган алгоритмлар асосида яратилган илк дастурий таъминот бўлиб, қуйидаги асосий вазифаларни бажаради:

— давлат ва тижорат корхоналарининг локал ва корпоратив тармоқлари орқали ҳимояланган электрон ҳужжат алмашувини бошқариш;

— Республикамизда ишлаб чиқилган «Электрон рақамли имзо» тўғрисидаги, «Электрон ҳужжат айланиши» тўғрисидаги қонунлар, ахборот ва коммуникация йўналишидаги дастурларни ҳаётга татбиқ этиш;

марказлашган электрон ҳужжат алмашиш тизимини яратиш.

Е-ҲУЖЖАТ қуйидаги имкониятларни яратади:

— электрон ҳужжатларни электрон рақамли имзо, шифрлаш, калит алмашиш тизимлари орқали махфийлигини ва бутунлигини таъминлаш;

— электрон ҳужжатларни марказлашган ҳолда сақлаш, алмашиш ва фойдаланувчиларнинг ишларини енгиллаштириш;

— фойдаланувчиларнинг шахсий ҳужжатларини шифрланган ҳолда сақлаш;

— фойдаланувчилар калитларини ва калит сертификатларини марказлашган ҳолда бошқариш.

Ушбу тизимда қўлланилган электрон ракамли имзо алгоритми давлат стандартига тўлиқ жавоб беради. Шифрлаш тизими 5-бўлимда ишлаб чиқилган алгоритм асосида яратилган. Калит алмашиш тизими эса 6-бўлимда келтирилган Диффи-Хэллман усулига ёндашув асосида такомиллаштирилган алгоритм бўйича яратилган. Дастурий таъминотда қўлланилган шифрлаш алгоритми Celeron 1.7 процессор, 256 Мб хотирага эга бўлган компьютерда 18 Мбит/сек гача тезликда ишлаши тажрибаларда аниқланган.

Е-ҲУЖЖАТ электрон ҳужжат алмашиш тизими сервер қисмидан ва фойдаланувчининг дастурий криптографик модулидан иборат. Сервер қисмининг асосий вазифаларига фойдаланувчиларни рўйхатдан ўтказиш, турли гуруҳларни ташкиллаштириш, аутентификация қилиш, очиқ калитларни ёки сертификатларни шифрланган ҳолда узатиш, сақлаш ва рўйхатга олиш, умумий ҳужжатларни сақлаш ва эгасига етказиб бериш киради. Фойдаланувчиларнинг дастурий криптографик модули эса, асосан, электрон ҳужжат ҳосил қилиш, электрон рақамли имзони шакллантириш ва уни текшириш, ҳужжатларни шифрлаш, ёпиқ калитларни ҳосил қилиш, шахсий ҳужжатларни ҳимояланган ҳолда сақлаш, ҳужжатларни жўнатиш ва қабул қилиш вазифаларини бажаради.

Е-ҲУЖЖАТ ва Е-ХАТ тизимларидан, Электрон рақамли имзо калитларини рўйхатга олиш марказидан, масофавий солиқ ҳисоботи топшириш тизими учун ишлаб чиқилган криптопровайдерлардан кўпгина корхоналарда, жумладан — Ўзбекистон алоқа ва ахборотлаштириш агентлиги, Давлат солиқ қўмитаси, Ташқи ишлар вазирлиги, Давлат алоқа инспекцияси, Фан-техника ва маркетинг тадқиқотлари маркази, Ўзимпексалоқа корхонаси, Ўзбектелеком АК ва бошқаларда фойдаланилмоқда.

6-бўлим бўйича хулосалар

1. Ишлаб чиқилган *носимметрик криптотизимларни диаматрица-устунлар алгебралари ҳамда параметрли алгебра асосида яратиш усули* криптотизим яратиш усулига асосий прототип танлашдан, прототипда фойдаланилган чекли бутун сонлар майдони устида берилган матрица-устунлар тўплами устида амалларни диаматрица-устунлар алгебрасининг параметрли амаллари билан, чекли бутун сонлар майдони устида берилган кўпайтириш амали асосида амалга ошириладиган даражага ошириш функцияларини ва бошқа амалларни параметрли алгебрада уларга мос параметрли кўпайтириш амали асосида параметрли даражага ошириш функциялари ва амаллари билан ҳамда тўпламларга тегишли бирлик ва ноллик элементларини мос тарзда ўзаро алмаштиришдан иборат. Мазкур усул асосида нафақат мавжуд носимметрик криптотизимларни алгебраик амаллар аналогиясидан фойдаланиб улардан кам бўлмаган криптобардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд носимметрик криптотизимларга нисбатан юқори криптобардошлиликка эга бўлган криптотизимлар яратиш имкониятини яратади.

2. Бир томонламалилик хусусиятига эга бўлган икки функция, яъни диаматрица-устунлар алгебраси ва параметрли алгебрада параметрли функция билан матрицавий параметрли функция кўплаб янги носимметрик криптотизимлар яратиш учун математик асос қилиб олиниши кўрсатиб берилди. Бир томонлама параметрли функциядан фойдаланиш мавжуд носимметрик криптотизимлар ўрнини боса оладиган криптотизимлар яратишда янгича ёндашувларга имкон беради. ЭРИ яратишга умумий схема усулида ёндашув амалга оширилиши мумкин бўлган схемалар кўламини бир неча баравар ошириш имконини беради.

3. Бир томонлама бутун сонли ва матрицавий параметрли функциядан фойдаланиб мавжуд криптотизимларни такомиллаштириш мумкинлиги RSA, Диффи-Хэллман, Ал Жамол ва Полиг-Хэллман усуллари бўйича ишлаб чиқилган ёки тако-

миллашган криптоалгоритмлар мисолида кўрсатиб берилди. Такомиллаштириш натижасида уларнинг криптобардошлилиги кескин ортади ва янги протоколлар ишлаб чикиш имкони туғилади. Ишлаб чиқилган криптотизимларнинг криптобардошлилиги махфий параметрлар ҳисобига мавжуд криптотизимларга нисбатан юқори бўлади. Уларни амалда қўллаш мумкинлиги муаллиф иштирокида ишлаб чиқилган Е-ҲУЖЖАТ электрон ҳужжат алмашиш тизими, Е-ХАТ электрон хат алмашиш тизими, Электрон рақамли имзо калитларини рўйхатга олиш маркази, масофавий солиқ ҳисоботини топшириш тизимининг ҳимоясида қўлланилган криптопровайдерлардан кўпгина корхоналарда, жумладан — Ўзбекистон алока ва ахборотлаштириш агентлиги, Давлат солиқ қўмитаси, Ташқи ишлар вазирлиги, Давлат алоқа инспекцияси, Фан-техника ва маркетинг тадқиқотлари маркази, Ўзимпексалоқа корхонаси, Ўзбектелеком АК ва бошқаларда фойдаланилаётганлиги исботлайди.

7-БЎЛИМ

ПАРАМЕТРЛИ АЛГЕБРАГА АСОСЛАНГАН НОСИММЕТРИК КРИПТОТИЗИМЛАРНИНГ КРИПТОБАРДОШЛИЛИГИ

7.1 Параметрли функциядан фойдаланишга асосланган криптотизимлар таҳлили мураккаблигининг қонуний ва ноқонуний томонлар учун ҳар хиллиги

Параметрли функциядан фойдаланишга асосланган криптотизимларнинг анъанавий бир томонлама даражага ошириш функциясидан фойдаланишга асосланган криптотизимлардан асосий фарқи шундаки, уларда параметр R дан фойдаланилади. Бунда параметр $R \geq 2^{160}$ қонуний томонлар учун маълум бўлса, ноқонуний томонлар учун номаълумдир. Бу албатта криптографик модуллар дастурий ва аппарат-дастурий кўринишда ишлаб чиқилган ҳолга тегишлидир. Агар криптографик модуллар ***махсус аппаратли модуль*** турига мансуб бўлса, унда махфий параметр R ваколатга эга субъект, масалан КРОМ томонидан ўрнатилиб криптографик модуль параметр R ҳақидаги ахборот ошкор бўлишидан муҳофаза қилиш механизмлари билан таъминланган бўлади. Тармоқ фойдаланувчилари, махфий параметр R ни билмаган тарзда криптографик модуллардан фойдаланганликлари туфайли, криптографик модулнинг бардошлилиги ва тезкорлиги нисбатан кичик ($p \sim 2^{256}$) модулларда ҳам қонуний ва ноқонуний томонлар учун етарлича юқори бўлади. Бундай махсус аппаратли модуллар Ўзбекистон алоқа ва ахборотлаштириш агентлиги қошидаги Фан-техника ва маркетинг тадқиқотлари маркази ходимлари томонидан, муаллиф иштирокида ишлаб чиқилмоқда. Қуйида, асосан ***дастурий*** **криптографик модуллар** устида сўз боради.

Даража параметри муаммосининг мураккаблигига асосланган криптотизимларда параметр R маълум бўлганда, даража параметри муаммосини дискрет логарифм муаммосига келтириш

мумкин бўлгани боис, бундай криптотизимларнинг криптобардошлилиги дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар криптобардошлилигига яқин, лекин ундан кам бўлмайди. Демак, қонуний фойдаланувчи томонлардан бири дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлсагина, криптотизимни обрўсизлантириш имконияти пайдо бўлади [21, 25, 26]. Яъни, қонуний фойдаланувчи томонлар орасида ўзаро ишонч бўлгандагина, даража параметри муаммосининг мураккаблигига асосланган криптотизимларнинг дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимларнинг криптобардошлилигидан кескин даражада юқори бўлади. Яъни, бунда криптотизимлар, асосан, ташқи бадният бузғунчиларга нисбатан криптобардошлиликни кескин даражада оширишга хизмат қилади.

Параметрли функциядан фойдаланишга асосланган криптотизимларда *ноқонуний томонлар* учун махфий саналган параметр R ни ҳисоблаб топиш учун энг қуйи — биринчи поғона мураккаблигига оид даража параметри муаммосини ҳал этиш учун 2.3.4-хоссага биноан

$$c \equiv \Sigma^{i=e-1}_{i=0} F^i \,(mod\ n) \qquad (7.1)$$

таққосламадан F ни ҳисоблаб топиш лозим;
бу ерда $c \equiv a^{-1} * a^{\backslash e} (mod\ n)$ маълум натурал сон.

Келтирилган таққослама $e = 3$ бўлганда $c \equiv \Sigma^{i=e-1}_{i=0} F^i \,(mod\ n)$ ифодаси $a^{-1} * a^{\backslash 3} \equiv 1 + F + F^2 \,(mod\ n)$ шаклини олади. Бу таққослама туб модулли ҳолларда иккинчи даражали таққосламага осонгина келтирилади ва масала квадрат илдизни топишдан иборат бўлади. Мураккаб модулли ҳолларда, квадрат илдиз топиш муаммоси факторлаштириш муаммосига тенг кучлидир.

Мураккаб модулли ҳоллар учун $e > 3$ бўлганда юқорида келтирилган алмаштиришларни бажаришдан аввал факторлаштириш муаммоси ҳал этилган бўлиши лозим. Бундай алмаштиришлар факторлаштириш муаммосига нисбатан қанчалик мураккаблиги ҳозирча тўла тадқиқ этилмаган. Бундан қатъий назар, даража параметри муаммоси факторлаштириш муам-

мосига нисбатан мураккаб, деган хулосага келиш мантиқан ўринлидир.

Туб модулли ҳолларда хам e туб сон бўлиб, $e>2^{159}$ бўлганда юқори даражали таққосламаларни ечиш мураккаб муаммодир. Бу e туб сон бўлганда $\Sigma^{i=e-1}_{i=0} F^i$ келтирилмайдиган кўпҳадлиги [99] билан ҳам боғлиқ. Шундай қилиб, даража параметри муаммосини қўпол куч усули билан ҳал этишдан бошқа усул ҳозирча муаллифга маълум эмас.

Туб модулли криптотизимлар учун R ни топиш эҳтимоллиги 2^{-q} га тенг бўлиб, $p>2^{160}$ бўлганда уни топиш имконияти амалда йўққа чиқади.

Даража параметри муаммосининг мураккаблигига асосланган криптотизимдан *қонуний фойдаланувчи томон*лардан бири дискрет логарифм муаммосини ечиш учун етарли ресурсларга эга бўлса, криптотизимнинг криптобардошлилиги асосан берилган модуль учун дискрет логарифм муаммосини ечиш сарф-харажатларига боғлиқ бўлади. Бунга қарши туриш учун дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимларга хос пухта модуллардан ($p>2^{1023}$) фойдаланиш лозим бўлади.

Юқорида билдирилган фикрлар параметрли функция асосида қурилган Полиг-Хэллман усулига асосланган шифрларга, Ал Жамол ва Диффи-Хэллман усулига мос махфий калит алмашиш криптотизимларига ҳамда ЭРИ умумий схемасига мос криптотизимларга тааллуқлидир.

Шуни таъкидлаш жоизки, даража параметри муаммосининг мураккаблигига асосланган криптотизимлар синфига оид барча ЭРИ умумий схемаларидан фойдаланилганда, махфий асосдан фойдаланилганлиги боис хам қонуний фойдаланувчи томонлар учун, ҳам ноқонуний фойдаланувчи томонлар учун криптотизимни обрўсизлантириш эҳтимоллиги икки марта пасаяди ва сеанс калитли маромда ЭРИ сохталигини пайқаш имконияти пайдо бўлади.

Факторлаштириш муаммосининг мураккаблигига асосланган RSA усулига мос шифр ва ЭРИ схемалари учун, *ноқонуний томонлар* учун махфий саналган параметр R ни то-

пиш эҳтимоллиги 2^{-n} га тенг. Ноқонуний томон криптотизимни обрўсизлантириши учун топилган параметр R дан фойдаланган ҳолда, яна модуль n учун факторлаштириш муаммосини ечиши ҳам лозим бўлади. Бинобарин, дискрет логарифм ёки факторлаштириш муаммосини ечиш имконияти бўлган ноқонуний томоннинг криптотизимни обрўсизлантириш эҳтимоллиги нолга яқин.

7.2 Электрон рақамли имзо схемалари криптотаҳлилини амалга ошириш йўналишлари

Даража параметри муаммосининг мураккаблигига асосланган барча ЭРИ умумий схемаларининг криптотаҳлил йўналишлари қуйидагиларга бўлинади. Булар [14]:

1. ЭРИ нинг ошкора калитларини сохталаштиришга йўналтирилган криптотаҳлил;
2. Ўзаро махфий калит — параметр R, R_{ij} ларни топишга йўналтирилган криптотаҳлил;
3. Электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш тақкосламаси асосида криптотаҳлил;
4. Хэш-функциянинг коллизиялар мавжудлигига асосланган ЭРИни сохталаштиришга йўналтирилган криптотаҳлил;
5. Ишлатиладиган протокол камчиликларидан фойдаланиш асосида имзони сохталаштиришга йўналтирилган криптотаҳлил.

Криптотаҳлилдан мақсад, имзо калитини билмаган ҳолда, алока канали бўйлаб жўнатилган сигналлар ўрнига аслига мос деб қабул қилинадиган бошқа мазмун бериб, ЭРИни ҳам сохталаштиришдир. Криптотаҳлилда одатда, биринчидан, имзоланган ҳужжат ва имзоловчининг идентификатори, иккинчидан, махфий имзо калитидан бошқа электрон рақамли имзо ва ошкора сеанс калитини шакллантириш ҳамда уни текширишга оид барча алгоритмлар ва протоколлар маълум деб ҳисобланади.

1-2-бандларда келтирилган криптотаҳлил турлари фақат даража параметри муаммосининг мураккаблигига асосланган ЭРИ схемалари учун хосдир, чунки ўзга электрон рақамли

имзо схемаларида ошкора калитлар ифодасида даража асоси ошкора параметр бўлиб, криптотаҳлилни мураккаблаштирувчи махфий асос ва параметр R, R_{ij} лар қатнашмайди. Бу ерда R_{ij} — махфий назорат калити. 3-бандда келтирилган криптотаҳлил тури ҳам, тасдиқлаш тақкосламасида махфий параметр R, R_{ij} лар қатнашиши туфайли, ўзининг мураккаблиги билан ажралиб туради. Электрон рақамли имзо дастурий таъминотидан фойдаланишда, ундан барча фойдаланувчилар ягона хэш-функция дастурий воситасига эга бўлишлари шарт бўлгани туфайли ҳужум объектлари қаторига хэш-функция дастурий воситаси ҳам киритилган. Қуйида хэш-функция дастурий воситаси зарур сифатларга эга ва ишлатиладиган протокол камчиликлардан ҳоли деб қаралган.

1-3-бандларга оид криптотаҳлил усуллари криптотаҳлил объекти синфининг моҳиятига кўра, қўпол куч асосида ва даража параметри муаммосини ечишга қаратилган криптотаҳлил жараёнлари кетма-кетлигидан иборат. Чунки, даража параметри муаммосини қўпол куч усулидан бошқа усул бўйича ечиш ҳозиргача маълум эмас. Даража параметри муаммосини ечиш, аввало, қўпол куч усули асосида махфий параметр R, R_{ij} ларни топишга, сўнгра даража параметри муаммосини дискрет логарифм муаммосига айлантириб, уни ечишга келтирилади.

Аввал айтиб ўтилганидек, ЭРИ умумий схемаларининг дастурий воситаларидан уч маромда фойдаланилади. Уччала маромда ҳам электрон рақамли имзони сохталаштириш учун параметр R, R_{ij} ларни топиш шарт. Фақат, R_{ij} ўрнида қонуний фойдаланувчилар учун ошкора параметр R_j дан фойдаланилганда масала соддалашади.

Шуни таъкидлаш керакки, рақиб томон криптотаҳлилчиси дискрет логарифм муаммосини еча олганда ҳам, сохталаштирилган электрон рақамли имзо икки қайта тасдиқлаш маромида барибир фош этилади. Бу ишлаб чиқилган рақамли имзо алгоритмининг энг кучли томонидир.

7.3 Электрон рақамли имзо криптотизими криптобардошлилигини баҳолаш

Носимметрик криптоалгоритмлар учун криптотаҳлил жараёнида уриниш амаллари сонининг ва уриниш натижасини синаш учун зарур бўлган амаллар сони сохта ошкора калитни (ва сеанс калитини) генерация қилиш учун зарур амаллар сони билан аниқланади [14] ва модуль узунлиги ошиши билан ночизиқли равишда ортиб боради.

Ишлаб чиқилган электрон рақамли имзо криптотизими учун криптотаҳлил объектлари бўлиб қуйидаги параметрлар хизмат қилади:

■ Биринчидан, имзоловчи шахсга тегишли калитлар. Булар юқорида қайд этилган криптотаҳлил йўналишлари рўйхатининг 1-3-бандларига оид қуйидаги параметрлардир:

1-объект: (x, u, x_1, a) — махфий калитлар тўртлиги — имзолаш калитлари; ошкора калитлар учлиги — (y, z, y_1) ни генерациялаш учун зарур бўлиб, буларнинг чин қийматлари топилса, имзони сохталаштиришга йўл очилиши мумкин, аммо $R > 1$ бўлганда бу етарли эмас, чунки $y \equiv a^{\backslash x} \ (mod\ p)$, $z \equiv a^{\backslash u} \ (mod\ p)$, $y_1 \equiv a^{\backslash x1} \ (mod\ p)$ ифодалари бўйича ҳисобланиб, ифодаларда даражага ошириш учун $R > 1$ параметри қўлланилади;

2-объект: R — ноқонуний фойдаланувчилар учун махфий параметр; у ошкора калитлар жуфтлигини генерациялаш ва ЭРИ ҳақиқийлигини дастлабки тасдиқлаш учун зарур;

3-объект: R_{ij} — ноқонуний фойдаланувчилар учун махфий бўлган назорат калити, унда R_{ij} имзоловчи шахс ва текширувчи томон учунгина маълум.

■ Иккинчидан, криптотаҳлил йўналишлари рўйхатининг 3-бандида келтирилган электрон рақамли имзо киради:

4-объект: (r, s) — жуфтлик — M хабарга қўйилган электрон рақамли имзо.

Криптотаҳлилчига 4-объектни сохталаштириш учун 1-, 2-, 3-объектлар маълум бўлиши лозим. Келтирилган криптотаҳлил объектлари орасида 1-, 2-, 3-объектлар энг юқори криптобардошлиликка эгадир, чунки уларни топиб олиш учун қўпол куч

усулидан фойдаланишга тўғри келади. Шундай қилиб, ҳар бир объектни сохталаштириш учун бир марта ёки ундан ортиқ қўпол куч усулидан фойдаланишга тўғри келади.

1-объектни ташкил этувчи компонентлар x, u, x_1, a ни тўғридан-тўғри танлов усулида топиш эҳтимоллиги 2^{-q} га тенг.

Криптотаҳлилчи a ни излашда қуйидаги стратегиядан фойдаланиш қулай бўлиши мумкин:

1-қадам: агар параметр R берилган бўлса, ошкора калитларнинг қийматини даража кўрсаткичли қийматлар y', z', y_1' га алмаштиринг, акс ҳолда R ни 2^q фазосидан топинг. Бунинг учун

2-қадам: ихтиёрий x' ни танланг;

3-қадам: $x'' \equiv x'^{-1} \pmod q$ ни ҳисобланг;

4-қадам: $a' \equiv y'^{x''} \pmod p$ ни ҳисобланг;

5-қадам: $y'' \equiv a'^{x'} \pmod p$ ни ҳисобланг;

6-қадам: $y'' == y'$ текширилади, агар тенглик бажарилса, унда a' параметр R га мос бўлган a билан алмаштирилади, акс ҳолда 2- қадамга қайтилади.

7-қадам: ихтиёрий u' ни танланг;

8-қадам: $z'' \equiv a'^{u'} \pmod p$ ҳисобланг;

9-қадам: $z'' == z'$ текширинг, агар тенглик бажарилса, унда ҳисоблашларни тўхтатинг, акс ҳолда 7- қадамга қайтинг.

10-қадам: ихтиёрий x_1' ни танланг;

11-қадам: $y_1'' \equiv a'^{x1'} \pmod p$ ҳисобланг;

12-қадам: $y_1'' == y_1'$ текширинг, агар тенглик бажарилса, унда ҳисоблашларни тўхтатинг, акс ҳолда 10- қадамга қайтинг.

1-объектни ташкил этувчи компонентлар x, u, x_1, a ни тўғридан-тўғри танлов усулида топиш эҳтимоллиги 2^{-q} га тенг.

Агар бадният бузғунчи ёки рақиб томон криптотаҳлилчиси қонуний фойдаланувчилар орасида бўлиб, дискрет логарифм муаммосини ечишга қодир бўлса, айниқса туб модуль сифатида $p \sim 2^{256}$ дан фойдаланилганда, R ва R_1 лар маълум бўлганда ва дастурий, анъанавий аппарат ёки аппарат-дастурий криптографик модулдан фойдаланилса, 1-объектни ташкил этувчи компонентлар x, u, x_1, a ни *аниқ ҳисоблаб топиш мумкин.* Бунда, бошланғич маълумот сифатида ЭРИ нинг барча ошкора пара-

метрлари, имзоланган маълумот M нинг хэш-қиймати m, ЭРИ (r, s, y_i), R ва R_1 лар бузгунчига маълум деб ҳисобланади.

1-объектни ташкил этувчи компонентлар x, u, x_1, a ни топиш учун қуйидаги қадамлар кетма-кетлигини амалга ошириш лозим.

1-қадамда қуйидаги

$$y \equiv z^{u} \pmod{p}, \tag{7.1}$$

$$y \equiv (m^{-1} \cdot r)^{y} \pmod{p} \tag{7.2}$$

иккита таққосламалар тизими билан берилган тизимни дискрет логарифм масалалари тизимига келтириш [25].

2-қадамда логарифм масаласи тизимини ечиш, яъни i ва j ни топиш.

3-қадамда i, j ва s учун ночизиқли таққосламалар тизимини қуйидаги

$$i \equiv x \cdot u^{-1} \pmod{q} \tag{7.3}$$

$$j \equiv x \cdot (-k)^{-1} \pmod{q}, \tag{7.4}$$

$$s \cdot u \equiv k - r \cdot x \pmod{q} \tag{7.5}$$

кўринишда тузиш.

4-қадамда i, j ва s учун ночизиқли таққосламалар тизимини ечиш ва x, u, k ларни топиш. Бу қадамни бажариш мураккаблиги дискрет логарифм масаласини ечишга қараганда бир неча маротаба осон.

5-қадамда $ut = u^{-1}$ қабул қилиб, $a \equiv z^{ut} \pmod{p}$ таққосламадан a топиш.

Натижада, сохта имзони шакллантириш имконияти туғилади. Бироқ, сохта ЭРИ давлат стандарти O‘z DSt 1092:2005 га хос НСКУ [100]га асосланган протоколга мувофиқ фойдаланувчига, сеанс назорат калити (y_1, a^{-k}) эса КРОМ орқали фойдаланувчиларга етказилиши туфайли, сохта ЭРИ бузғунчининг ўзигагина тегишли қилиб КРОМ ЭРИ си билан тасдиқланади. Фойдаланувчи эса ЭРИ ҳақиқийлигини тасдиқлаш жараёнида бузғунчининг ошкора калитларидан фойдаланади ва ЭРИ ни ҳақиқий эмас, деган хулосага келади. Чунки бузғунчига ҳақиқий ЭРИ эгасининг КРОМ билан боғланишда фойдаланадиган махфий симметрик калит маълум эмас ва у (y_1, a^{-k}) ни фақат ўзининг махфий симметрик калити билан шифрлаб

КРОМга жўнатиши мумкин. Натижада, протокол туфайли, криптотаҳлилчининг сохталаштирилган электрон рақамли имзоси фош бўлиб, ракиб томон криптотаҳлилчисининг меҳнати зое кетиши туфайли бузғунчи бундай ҳужум стратегиясидан фойдаланмайди. Бузғунчи бундай стратегиядан, қонуний ЭРИ эгасининг КРОМ билан боғланадиган махфий симметрик калитини қўлга киритган бўлсагина, фойдаланиб ўз мақсадига эришиши мумкин. Бундай имконият ҳар қандай ЭРИ схемасига тенг тааллуқлидир.

2-объект R топиш эҳтимоллиги ва 3-объект R_{ij} ларни топиш эҳтимоллиги 2^{-q}. Бинобарин, юқорида санаб ўтилган махфий параметрларни топиш учун ўлчамлари $q = 2^{255}$ бўлган улкан фазода кетма-кет танлаш усулини қўллаш лозим бўлади. Маълумки, яқин келажакда буни мавжуд ҳисоблаш техникаси воситалари ёрдамида амалга ошириш имконияти мавжуд эмас.

4-объектни сохталаштириш учун криптотаҳлилчи дастлаб текшириш ифодасидаги ҳакикий ҳужжат хэш-функцияси қиймати m ни сохта ҳужжатнинг хэш-функцияси m' билан алмаштирилган ифодани шакллантиради, сўнгра дискрет логарифм муаммосини ечиш натижасида сохта имзонинг биринчи қисми s' ни топади. Яъни, криптотаҳлил қуйидаги қадамлар кетма-кетлигини бажаришдан иборат:

1-қадам: $m' \equiv z^{s}\,®\,y^{r}\,®\,r \pmod p$ шакллантиринг; бу ерда $r_1 = r \pmod q$.

2-қадам: $z^{s'} = m'\,®\,y^{-r}\,®\,r^{-1} \pmod p$ ҳисобланг; бу ерда $y^{-r} \pmod p$ — y^{r} нинг p модуль бўйича диатескари қиймати, $r^{-1} \pmod p$ — r нинг p модуль бўйича параметрли тескари қиймати.

3-қадам: $z^{s'}$ нинг қийматига мос $z^{s'}$ қиймат билан алмаштиринг.

4-қадам: дискрет логарифм муаммосининг ечими сифатида s' ни топинг.

Оқибатда, сохта ҳужжат хэш-функцияси m' учун мос сохта имзо $(r; s')$ ни шакллантиради. Бунда ҳар бир ҳақиқий имзони сохталаштириш учун ҳар сафар янгидан дискрет логарифм муаммосини тўла ечиш зарур бўлади.

Шундай қилиб, махфий калитлар x, u, x_1, махфий асос a ни дискрет логарифм масаласи асосида ҳисоблаш учун, аввало махфий параметр R, назорат калити R_{ij} маълум бўлиши даркор; улардан ҳар бирини ҳисоблаб топиш учун $5,79*10^{76}$ амални бажариш зарур ва бу $1,93*10^{63}$ mips — йилни ташкил қилади.

Бинобарин, ишлаб чиқилган электрон рақамли имзо дастурий таъминоти юқори криптобардошлилик талабига жавоб беради.

7-бўлим бўйича хулосалар

1. Қонуний ва ноқонуний фойдаланувчилар учун даража параметри маълум бўлса, унда ишлаб чиқилган криптографик тизимларнинг криптобардошлилиги мавжуд криптотизимларники каби бўлади. Агар даража параметри R фақат битта субъектга маълум бўлиб, бошқа барча қонуний фойдаланувчилардан сир сақланса, криптографик тизим криптобардошлилиги $R \geq 2^{160}$ бўлганда мавжуд криптотизимларникига нисбатан етарлича юқори бўлади. Бу имконият криптографик модулларнинг махсус аппаратли модуль турига хосдир. Бундай криптографик модулларда параметр R криптографик модулга фақат ваколатга эга субъект томонидан ўрнатилиб, криптографик модуль параметр R ҳақидаги ахборот ошкора бўлишидан муҳофаза қилиш механизмлари билан таъминланган бўлади. Дастурий ва аппарат-дастурий кўринишда тайёрланган криптографик модуллар бундай имкониятларга эга эмас.

2. Махфий калитлар x, u, x_1, махфий асос a ни дискрет логарифм масаласи асосида ҳисоблаш учун, аввало махфий параметр R, назорат калити R_{ij} маълум бўлиши даркор; улардан ҳар бирини ҳисоблаб топиш учун $5,79*10^{76}$ амални бажариш зарур ва бу $1,93*10^{63}$ mips — йилни ташкил қилади. Бинобарин, ишлаб чиқилган электрон рақамли имзо дастурий таъминоти юқори криптобардошлилик талабига жавоб беради.

ХУЛОСА

Ушбу китобда шу кунга қадар дунёда кенг тарқалган ва энг пухта деб тан олинган кўпгина симметрик ва носимметрик криптотизимлар, уларни яратишга асос бўлган алгебраик структуралар ва функциялар қисқача ёритиб берилди. Ошкора криптография юзага келгандан буён туб ва мураккаб модулда ягона махфийликка (махфий йўлга) эга бўлган даражага ошириш функцияси ошкора криптографиянинг асосий бир томонлама функцияси бўлиб қолмоқда.

Муаллиф томонидан такомиллаштирилган диаматрицалар алгебраси, диаматрица-устунлар алгебраик структураси, бутун сонли ва матрицавий параметрли алгебраик структуралар, алгебраик амаллар ҳамда функциялар хоссалари мавжуд криптотизимларни такомиллаштириш усулларининг яратилиши билан бир қаторда, янги даража параметри муаммоси ва унга мос Диффи-Хэллман муаммоларини юзага чиқарди, дискрет логарифм ва факторлаштириш муаммосига муқобилли ёндашувларга йўл очилди.

Шифрлар яратишда анъанавий матрицалар алгебраси ўрнига ёки биргаликда такомиллашган диаматрицалар алгебрасидан шифралмаштиришларда киришда битта элемент ўзгариши чиқишда матрицавий кўпайтма чиқишидагига нисбатан *1,5-1,75* марта кўп элементлар ўзгаришига олиб келиши асос бўлади. Бу хосса шифрлаш босқичлари сонини камайтиришга, бинобарин, шифрлаш тезлигини ёки боскичлар сони ўзгармаганда, криптобардошлиликни оширишга хизмат қилади.

2 хил модуль $n \in \{p, p_1 * p_2\}$ бўйича параметрли функциянинг хоссалари фойдаланиш йўналиши бўйича 2 синфга — криптография ва криптотаҳлил синфларига ажратилди. Шунингдек, Эйлер пи-функцияси атамасининг кенгайтирилган изоҳи берилди.

Модуль n, параметр R билан p, p_1 ёки p_2 ўзаро туб бўлса "Эйлер пи-функцияси $\varphi(n)$ қиймати" атамасидан фойдаланиш тўғри эмаслиги, Эйлер пи-функцияси $\varphi(n)$ қиймати деганда n билан ўзаро туб сонлар назарда тутилиши боис, бу қиймат кел-

тирилган анъанавий ифода бўйича ҳисоблаш натижасидан кам чиқиши аниқланди. Аслида бу атама "Вазифаси бўйича Эйлер пи-функцияси $\varphi(n)$ киймати аналоги" маъносини ифода этиши аниқланди. Мазкур ҳолат параметрли функциянинг бошқа бир томонлама функциялардан тамойилли фарқини тасдиқлайди.

Матрицавий параметрли функциянинг хоссалари мажмуида матрицавий экспоненциал функция хоссаларига ўхшаш томонлари ҳам, ундан фарқли томонлари ҳам мавжуд. Ўхшаш томонлар биртомонлама матрицавий параметрли функция асосида барча биртомонлама матрицавий дискрет даражага ошириш функцияси асосида ишлаб чиқилиши мумкин бўлган криптотизимларни такомиллаштириш имконини беради. Фарқли томонлар матрицавий параметрли функция асосида мавжуд криптотизимлардан тамойилли фаркли криптотизимлар яратишга ва криптотаҳлилга янгича ёндашувларга замин яратади.

Бир томонлама параметрли функция хоссаларидан келиб чиққан учта мураккаблик поғоналарига бўлинган даража параметри муаммосига ўхшаш муаммо ҳисоблаш мураккаблигига оид нашрларда келтирилмаган. Агар даража параметри берилган бўлса, унда даража параметри муаммоси дискрет логарифм муаммосига, параметрли функциянинг хоссалари асосида осонгина келтирилади. Шунингдек, даража параметри муаммосига мос Диффи-Хэллман муаммоси R_1, R_2 маълум бўлсагина Диффи-Хэллман муаммосига, матрицавий даража параметри муаммосига мос матрицавий Диффи-Хэллман муаммоси эса $\underline{R}$ маълум бўлганда матрицавий Диффи-Хэллман муаммосига келтирилади.

Диаматрица-устунлар алгебраси ва параметрли алгебра асосида носимметрик криптотизимлар яратиш усули, шифр яратишга Полиг-Хэллман, RSA, Тоҳир Ал Жамол усулларида, электрон ракамли имзо криптотизимини яратишга эса RSA ва умумий схема усулларида, махфий калит алмашув алгоритмини яратишга Диффи-Хэллман усули асосида ёндашувлар баён этилди. Олиб борилган тадқиқотлар асосида, ҳимояланган Электрон ҳужжат ва хат алмашиш тизимлари «Е-ҲУЖЖАТ»

ҳамда «Е-ХАТ» ишлаб чиқилди, ундан ҳозирги кунда давлат ва нотижорат корхоналарида фойдаланилмоқда.

Китобда параметрли функциядан фойдаланишга асосланган криптотизимлар криптобардошлилиги таҳлили мураккаблигининг қонуний ва ноқонуний томонлар учун ҳар хиллиги, криптотаҳлилни амалга ошириш йўналишлари ва электрон рақамли имзо криптотизими криптобардошлилигининг баҳоси келтирилди. Қонуний ва ноқонуний фойдаланувчилар учун даража параметри маълум бўлса, унда ишлаб чиқилган криптографик тизимларнинг криптобардошлилиги мавжуд криптотизимларники каби бўлади. Агар даража параметри R фақат битта субъектга маълум бўлиб, бошқа барча қонуний фойдаланувчилардан сир сакланса, криптографик тизим криптобардошлилиги $R \geq 2^{160}$ бўлганда, мавжуд криптотизимларникига нисбатан етарлича юқори бўлади. Бу имконият криптографик модулларнинг *махсус аппаратли модуль* турига хосдир. Бундай криптографик модулларда параметр R криптографик модулга фақат ваколатга эга бўлган субъект томонидан ўрнатилиб, криптографик модуль параметр R ҳақида ахборот ошкор бўлишидан муҳофаза механизмлари билан таъминланган бўлади. Дастурий ва аппарат-дастурий криптографик модуллар бундай имкониятларга эга эмас.

Махфий калитлар ва параметрлардан ҳар бирини ҳисоблаб топиш учун $5,79*10^{76}$ амални бажариш зарур ва бу $1,93*10^{63}$ mips — йилни ташкил қилади. Бинобарин, ишлаб чиқилган электрон рақамли имзо дастурий таъминоти криптографик модулларга қўйилган юқори криптобардошлилик талабларига жавоб беради, деб хулоса чиқариш ўринлидир.

Муаллиф томонидан такомиллаштирилган диаматрицалар алгебраси, диаматрица-устунлар алгебраик структураси, бутун сонли ва матрицавий параметрли алгебраик структуралар криптографияда фойдаланиладиган алгебраик структуралар билан бир қаторда ўзининг муносиб ўрнига эга. Бу алгебраик структуралар бошқа соҳаларда ҳам, масалан кодлаш назариясида, электр ва электромагнит тизимларни эквивалент ва ноэквивалент алмаштиришларда ҳам кенг фойдаланилиши мумкин.

ИЛОВАЛАР

1-илова

Такомиллаштирилган диаматрицавий шифр алмаштириши учун кириш массиви элементи ўзгаришига мос чиқиш элементларининг ўзгариш соҳалари

Модуль $n=256$ учун 4-тартибли d_2-матрицаларнинг элементлари ўзгарганда натижавий матрицаларда ўзгариш соҳалари

а) Ўзгариш чап диаматрицада

$$A \quad B \quad C$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 135 & 15 & 113 & 227 \\ 255 & 82 & 9 & 80 \\ 107 & 141 & 8 & 206 \\ 73 & 84 & 241 & 201 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 10 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 12 & 107 & 218 \\ 169 & 83 & 13 & 86 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 15 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 16 & 115 & 230 \\ 255 & 83 & 9 & 80 \\ 193 & 139 & 10 & 200 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 15 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 15 & 113 & 227 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 116 & 83 & 239 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 7 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 164 & 76 & 184 \\ 19 & 83 & 44 & 120 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 10 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 88 & 14 & 111 & 224 \\ 3 & 113 & 16 & 88 \\ 107 & 141 & 3 & 206 \\ 73 & 84 & 241 & 196 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 19 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 14 & 111 & 224 \\ 7 & 83 & 23 & 96 \\ 99 & 201 & 10 & 190 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 21 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 14 & 111 & 224 \\ 11 & 83 & 30 & 104 \\ 107 & 141 & 10 & 206 \\ 61 & 174 & 220 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 5 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 250 & 181 & 200 \\ 255 & 83 & 9 & 80 \\ 125 & 161 & 10 & 230 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 22 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 14 & 111 & 224 \\ 246 & 83 & 44 & 68 \\ 116 & 151 & 10 & 218 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 7 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 83 & 14 & 111 & 224 \\ 255 & 73 & 9 & 80 \\ 116 & 151 & 45 & 218 \\ 73 & 84 & 241 & 192 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 30 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 116 & 151 & 10 & 218 \\ 64 & 74 & 20 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 5 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 92 & 0 & 96 & 7 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 86 & 98 & 0 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 1 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 92 & 14 & 111 & 224 \\ 242 & 83 & 250 & 119 \\ 107 & 141 & 10 & 206 \\ 86 & 98 & 0 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 32 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 94 & 127 & 10 & 245 \\ 86 & 98 & 0 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 10 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 79 & 14 & 111 & 224 \\ 255 & 69 & 9 & 80 \\ 107 & 141 & 251 & 206 \\ 86 & 98 & 0 & 243 \end{vmatrix}$$

b) Ўзгариш ўнг диаматрицада

$$\begin{matrix} & A & & & & & B & & & & & C & & \\ \begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} & & & & \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} & & & & \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix} \end{matrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 18 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 93 & 14 & 111 & 224 \\ 11 & 83 & 9 & 80 \\ 120 & 141 & 10 & 206 \\ 87 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 2 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 92 & 56 & 111 & 224 \\ 255 & 91 & 9 & 80 \\ 107 & 145 & 10 & 206 \\ 73 & 88 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 3 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 14 & 154 & 224 \\ 255 & 83 & 18 & 80 \\ 107 & 141 & 15 & 206 \\ 73 & 84 & 0 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 4 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 14 & 111 & 12 \\ 255 & 83 & 9 & 68 \\ 107 & 141 & 10 & 224 \\ 73 & 84 & 241 & 212 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 5 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 84 & 14 & 111 & 224 \\ 57 & 83 & 9 & 80 \\ 103 & 141 & 10 & 206 \\ 69 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 16 & 111 & 224 \\ 255 & 92 & 9 & 80 \\ 107 & 158 & 10 & 206 \\ 73 & 102 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 8 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 14 & 112 & 224 \\ 255 & 83 & 76 & 80 \\ 107 & 141 & 7 & 206 \\ 73 & 84 & 252 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 9 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 14 & 111 & 226 \\ 255 & 83 & 9 & 126 \\ 107 & 141 & 10 & 220 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

c) 2 элементга ўзгариш чап диаматрицада

$$\begin{matrix} A \\ \end{matrix} \quad \begin{matrix} \\ \end{matrix} \quad \begin{matrix} B \\ \end{matrix} \quad \begin{matrix} \\ \end{matrix} \quad \begin{matrix} C \\ \end{matrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 5 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 135 & 1 & 98 & 10 \\ 255 & 82 & 9 & 80 \\ 107 & 141 & 8 & 206 \\ 86 & 98 & 0 & 201 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 4 \\ 12 & 9 & 21 & 1 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 135 & 15 & 113 & 227 \\ 242 & 82 & 250 & 119 \\ 107 & 141 & 8 & 206 \\ 86 & 98 & 0 & 201 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 32 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 135 & 15 & 113 & 227 \\ 255 & 82 & 9 & 80 \\ 94 & 127 & 8 & 245 \\ 86 & 98 & 0 & 201 \end{vmatrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 10 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 122 & 15 & 113 & 227 \\ 255 & 68 & 9 & 80 \\ 107 & 141 & 249 & 206 \\ 86 & 98 & 0 & 240 \end{vmatrix}$$

d) Битта элемент ўзгарганда 2 босқичли шифрлаш

$$\begin{matrix} A \\ \begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \end{matrix} \circledR_2 \begin{matrix} B \\ \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \end{matrix} \equiv \begin{matrix} C \\ \begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix} \end{matrix}$$

$$\begin{vmatrix} 2 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 135 & 15 & 113 & 227 \\ 255 & 82 & 9 & 80 \\ 107 & 141 & 8 & 206 \\ 73 & 84 & 241 & 201 \end{vmatrix}$$

$$\begin{vmatrix} 135 & 15 & 113 & 227 \\ 255 & 82 & 9 & 80 \\ 107 & 141 & 8 & 206 \\ 73 & 84 & 241 & 201 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 232 & 40 & 49 & 127 \\ 124 & 199 & 91 & 215 \\ 90 & 85 & 5 & 29 \\ 188 & 49 & 235 & 26 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 13 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 15 & 113 & 227 \\ 42 & 83 & 7 & 77 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 92 & 15 & 113 & 227 \\ 42 & 83 & 7 & 77 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 114 & 40 & 49 & 127 \\ 242 & 210 & 243 & 1 \\ 90 & 85 & 109 & 29 \\ 188 & 49 & 235 & 240 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 14 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 15 & 113 & 227 \\ 255 & 83 & 9 & 80 \\ 150 & 140 & 10 & 203 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 92 & 15 & 113 & 227 \\ 255 & 83 & 9 & 80 \\ 150 & 140 & 10 & 203 \\ 73 & 84 & 241 & 204 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 114 & 40 & 49 & 127 \\ 124 & 210 & 91 & 215 \\ 208 & 74 & 109 & 71 \\ 188 & 49 & 235 & 240 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 15 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 92 & 16 & 115 & 230 \\ 255 & 83 & 9 & 80 \\ 193 & 139 & 10 & 200 \\ 73 & 84 & 241 & 204 \end{vmatrix}$$

$$\begin{vmatrix} 92 & 16 & 115 & 230 \\ 255 & 83 & 9 & 80 \\ 193 & 139 & 10 & 200 \\ 73 & 84 & 241 & 204 \end{vmatrix} \circledR_2 \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} \equiv \begin{vmatrix} 114 & 51 & 153 & 85 \\ 124 & 210 & 91 & 215 \\ 70 & 63 & 109 & 113 \\ 188 & 49 & 235 & 240 \end{vmatrix}$$

2-илова

Маълумот алмашиш протоколлари

2.1 Протоколлар

Криптоалгоритмларни амалиётга татбиқ этиш протоколлар асосида рўй беради. Криптотизим протоколи криптоалгоритмнинг ахборот хавфсизлигини таъминлашни кафолатлашга хизмат қилувчи қоидалар ва тартиботлар (аниқ амаллар кетма-кетликлари) мажмуидир. Унинг воситасида икки ёки ундан кўп томонлар биргаликда муайян вазифани ижро этадилар. Бунда ҳар бир ҳаракат бошидан охиригача навбатма-навбат бажарилади. Криптотизим, бардошли криптоалгоритмга эга бўлиши билан бир қаторда, ишончли пухта протоколга ҳам эга бўлиши шарт. Протоколлар туфайли ахборот хавфсизлигига бўладиган тажовузларнинг оқибати симметрик криптотизимларга ҳам, ошкора калитли (носимметрик) криптотизимларга ҳам хосдир.

Ошкора калитли криптотизимларнинг дастлабки пайдо бўлган даврларида ишлаб чиқилган протоколларга қатор камчиликлар хос бўлган. Бардошли криптоалгоритмлар қўлланганда ҳам протокол туфайли криптотизимнинг ахборот хавфсизлиги таъминланмаган. Пухта бўлмаган протоколларга хос бўлган камчиликларга қуйидагилар киради:

1. Имзо қўйилиб тасдиқланадиган ҳужжат шаклига қўйиладиган талабнинг бўшлиги;
2. Умумий модулдан фойдаланиш;
3. Кичик қийматли ошкора калит ишлатиш;
4. Энтропияси кичик бўлган хабарлар маконидан фойдаланиш.

Бу заифликлар RSA криптотизимининг айрим протоколларига хос бўлиб, у Ж. Мур RSA криптотизимида ишлатиладиган протокол, агар барча фойдаланувчилар учун модуль M бир хил олинса ёки ошкора калит тарзида кичик сон олинса, ёки бўлмаса шифрланаётган ахборотнинг энтропияси кичик (бу ҳол айниқса телефон сўзлашувлари учун хос) бўлса, шифр-

ни бузиб очиш осонлигини кўрсатиб ўтган. Ҳар қандай криптотизимни яратишда ишлаб чиқиладиган протокол бузғунчи қўллаши мумкин бўлган барча ҳолларни ҳисобга олган ҳолда мукаммал бўлиши лозим. Криптографик протоколларни бардошли деб ҳисоблаш учун уни ишлатиш жараёнида қонуний фойдаланувчилар ўз мақсадларига эришишлари, бузғунчилар эса эриша олмасликлари шарт.

Протокол қуйидаги талабларга жавоб бериши лозим:

1. Ҳар бир протокол иштирокчиси протоколни ва протоколдаги барча ҳаракатларни билиши;

2. Ҳар бир протокол иштирокчиси протокол кетма-кетлигига рози бўлиши;

3. Протокол икки маъноли бўлмаслиги — ҳеч қандай тушунмовчиликлар юзага келмаслиги учун ҳар бир ҳаракат аниқ ёритилиши;

4. Протокол тўлиқ бўлиши — унда ҳар қандай вазият ҳисобга олиниб, ҳаракатлар аниқ кўрсатилиши керак.

Томонлар бир-бирига ишониши ва бир-бири билан дўст бўлиши мумкин ва аксинча, икки томон бир-бирига, ҳаттоки, душман бўлиб, ташқаридан келадиган хабарни муайян вақт мобайнида бир-биридан яшириши ҳам мумкин. Криптографик протокол бир нечта криптографик алгоритмларни (дастурларни) қўллаган ҳолда амалга оширилади, аммо протоколлар фақат махфийликни таъминлаш учунгина мўлжалланган эмас.

Протоколда кўрсатилгандан ортиқ нарсани билиш ва бажариш мумкин эмас. Айрим протоколларда иштирокчилар бир-бирини алдаши мумкин. Бошқа протоколларда бадниятли кишилар протоколни бузиши мумкин ёки махфий маълумотларни билиб олиши мумкин. Протоколнинг пухталигини билиш, протоколнинг пухта эмаслигини исбот-лашга қараганда анча осондир.

Тадқиқотчилар учун протоколлар пухталигини текшириш асосий вазифа бўлиб ҳисобланади. Криптографик протоколлар таҳлили учун тўртта асосий нуқтаи назар маълум:

1. Махсус тиллар ва синаш воситаларидан фойдаланиш орқали протокол ишини текшириш ва моделлаш; бундай

йўл криптографик протоколлар таҳлили учун махсус ишлаб чиқилган бўлиши шарт эмас.

2. Протокол ишлаб чиқувчи учун турли сценарийларни тадқиқ қилиш ва яратишга имкон берувчи эксперт тизимларни ишлаб чиқиш.

3. «Билим» ва «ишонч» тушунчаларининг таҳлили учун формал мантиқдан фойдаланиб, протоколлар оиласи учун талаблар ишлаб чиқиш.

4. Алгебраик шаклдаги криптографик тизимлар хоссалари ёзувига асосланган формал усуллар ишлаб чикиш.

Протоколлар қуйидаги гуруҳларга бўлинади:

Воситачили протокол

Воситачили протоколларнинг камчиликлари:

1. Бир-бирига шубҳа билан муносабатда бўлган икки томон воситачига ҳам шундай шубҳа билан муносабатда бўлиши мумкин;

2. Компьютер тармоғи воситачини қўллаб-қувватлашни таъминлаши керак;

3. Ҳамма воситачили протоколларда кечикиш мавжуд;

4. Воситачи ҳар қандай протоколнинг йирик масштабли амалга оширишларида тор ўрин деб ҳисобланувчи ҳар бир трансакциясида иштирок этиши керак;

5. Тармоқда ҳар ким воситачига ишониши керак, акс ҳолда воситачи тармоқда уни бузишга бўлган уринишларда заиф ўринни эгаллайди.

Арбитрли протокол

Арбитрли протоколни қуйи поғонали икки нимпротоколга ажратиш мумкин. Биринчиси воситачисиз протокол бўлиб, томонларнинг хоҳишлари билан қўлланилади. Бошқаси эса воситачили протокол бўлиб, томонларнинг тушунмовчиликлари натижасида амалга оширилади. Махсус воситачи арбитр деб аталади.

Ўзиетарли протокол

Ўзиетарли протокол протоколнинг энг яхши тури ҳисобланади. Лекин ҳар бир ҳолатлар учун ўзиетарли протоколлар мавжуд эмас.

Протоколга қарши ҳужум турларига қуйидагилар киради:

1. Суст ҳужум (ахборот олиш мақсадида протоколларни эшитиш).

2. Фаол ҳужум (протоколни ўзгартиришга уринишлар — хабарни ўзгартириш, қўйиш).

3. Суст фирибгарлар ҳужуми, яъни томонлардан бири протоколни таъқиб қилишни тўхтатмаган ҳолда кўпрок ахборот олишга ҳаракат қилиши.

4. Фаол фирибгарлар ҳужуми, яъни томонлардан бири протоколни ўзгартириши мумкин.

2.2 Протокол тузишда прототипнинг роли

Ишлаб чиқилган маълумотларни шифрлаш тизими (алгоритмик ва дастурий таъминоти) учун протокол тузишда ҳам унинг учун прототип вазифасини ўтайдиган стандартлардан фарқли томонларни ҳисобга олиш зарур. Бу мавжуд стандартларда қўлланиладиган протоколларнинг кучли томонларидан фойдаланишга имкон яратади.

Ишлаб чиқилган маълумотларни шифрлаш алгоритми учун прототип вазифасини АҚШ стандарти AES ўташи мумкин.

И2-жадвалда ишлаб чиқилган маълумотларни шифрлаш алгоритми (МША) ва АҚШ стандарти AES учун протокол мазмунига ва криптобардошлиликка таъсир кўрсатиши мумкин бўлган қиёсий кўрсаткичлар келтирилган.

И2-жадвал

МША ва AES алгоритмларининг қиёсий кўрсаткичлари

Кўрсаткич	*МША*	*AES*
Блок узунлиги, бит	*128, 256*	*128*
Шифрлаш калити узунлиги, бит	*128, 256*	*128, 192, 256*
Функционал калит узунлиги, бит	*128, 256*	—
Функционал калитнинг янгиланиш тартиби	*Сеанслар сони бўйича*	—
Функционал калитни янгилаш функцияси	*Хэш-функция*	—
Раунд калити ўзгаришининг боғлиқлиги	*Функционал калитга*	*Шифрлаш калитига*
Аралаштириш ўзгартиришида ишлатиладиган матрица тури	*Махфий; функционал калитга боғлиқ*	*Ошкора, доимий*
Байтлаб алмаштиришда фойдаланиладиган жадвал	*Махфий; функционал калит ва раундга боғлиқ*	*Ошкора, доимий*

Келтирилган жадвалдан кўриниб турибдики, МШАда AESдан фарқли ўлароқ, раунд (босқич) калитларини ҳосил қилиш учун даврий янгиланиб турадиган қўшимча калит — функционал калитнинг қўлланилишидир. Бу нафақат раундлар сонини камайтиришга, балки ҳар гал янги функционал калит қўлланилганда раунд калитларини ҳам батамом янгилашга, бинобарин, асосий ўзгартиришлар бўлган аралаштириш ўзгартиришида ишлатиладиган ҳамда байтлаб алмаштиришда фойдаланиладиган диаматрицаларни янгилаш ва уларни махфийлаштиришга имконият яратади. Бу эса AESга нисбатан криптотаҳлилчининг ишини кескин мураккаблаштириб, МША криптобардошлилигини сезиларли оширувчи омилдир.

Функционал калитни янгилаш учун ишлатиладиган хэш-функция дастури фойдаланувчига аталган дастурий таъминотда келтирилган бўлиши лозим. Уни янгилаш фойдаланувчилар жуфтлари ўзаро келишиб олган муддатларда бажарилади. Бун-

да шифрланадиган ҳужжатнинг махфийлик даражаси албатта ҳисобга олиниши шарт. Махфийлик даражаси канчалик юқори бўлса, функционал калит шунчалик тез янгиланиб бориши лозим бўлади.

Протокол бошлангунча икки ҳол бўлиши мумкин:

1. Фойдаланувчилар жуфтида битта калит, яъни шифрлаш калити мавжуд.

2. Фойдаланувчилар жуфтида иккита, бир-биридан мустақил бўлган калитлар, яъни шифрлаш калити ва дастлабки функционал калит мавжуд.

Функционал калитни *i*-сеанс учун янгилаш жараёнида фойдаланиладиган хэш-функциянинг хэшлаш калити тарзида шифрлаш калити, кириши сифатида $i > 1$ бўлганда $(i-1)$-сеанс учун фойдаланилган функционал калит ишлатилади. Биринчи сеансда кириш сифатида дастлабки функционал калит берилганда унинг ўзи, акс ҳолда шифрлаш калити ишлатилади. Қуйида шу иккала ҳол учун тузилган протоколлар келтирилган.

2.3 Маълумотларни шифрлаш протоколлари

Маълумотларни шифрлаш криптотизими протоколи ахборот хавфсизлигини таъминлашни кафолатлаш тамойилларига мувофиқ белгиланган аниқ амаллар кетма-кетлиги кўринишида тавсиф этилиб, унга биноан икки ёки ундан кўп томонлар биргаликда иш юритадилар. Бунда ҳар бир амал бошидан охиригача навбатма-навбат бажарилади ва томонлар фойдаланиладиган шифрлаш мароми ва функционал калитни янгилаш тартиби ҳақида келишиб олишлари лозим. Қуйида келтирилган протоколлар МША дастурий таъминоти Elektron kod kitobi (*EKK*) ва Shifr Bloklarni ilaktirish (*SBI*) (русча, сцепление блоков шифра) маромлари учун мўлжалланган. Маълумотларни шифрлаш протоколида иштирок этувчи томонлар биринчи (*B*) ва иккинчи (*I*) лардир.

1-протокол. Бир калитли маром учун шифрлаш протоколи

Протоколни бажариш бошлангунча *B* ва *I* томонлар учун сертификацияланган бир хил МША дастурий таъминотига, хэш-функция *h* ни ҳисоблаш дастурига, шунингдек, *I* томон *B* томон билан биргаликда махфий шифрлаш калити *k* га эга ва *B* томон шифрлаши учун дастлабки ҳужжат *M* берилган деб ҳисоблаймиз. Шу билан бир қаторда, томонлар функционал калитни янгилаш тартиби ва шифрлаш мароми тўғрисида ҳам келишиб олганлар, деб ҳисобланади. Бунда *B* ва *I* томонларга тегишли сертификатланган бир хил дастурий таъминот, хэш-функцияни ҳисоблаш дастури ва махфий шифрлаш калити ишончли воситачи ёки калитлар алмашиш ошкора криптотизими ёрдамида етказилиши мумкин.

1. *B* томон хэш-функция дастуридан фойдаланиб, хэш-функциянинг хэшлаш калити сифатида шифрлаш калити *k* ни қабул қилиб, функционал калит $k_f = h(x)$ ни ҳисоблайди. Агар жорий сеанс биринчи бўлса, унда хэш-функциянинг кириши $x=k$ ва акс ҳолда $x=k_{f-1}$, бу ерда k_{f-1} — олдинги сеансда ишлатилган функционал калитдир.

2. *B* томон шифрланадиган ҳужжат *M* ни иккилик саноқ тизимига келтириб, уни узунлиги *128* (*256*) битли $n \geq 1$ блокларга ажратади. Агар сўнгги блок *128* (*256*) битдан кам бўлса, унинг охирига "блок охири" ишоратини қўйиб, қолган бўш хоналарни *01* лардан тузилган кетма-кетлик билан тўлдиради. Бунда *0* ва *1* рақамлари галма-гал алмашиб боради. Натижада *M* га мос кириш кетма-кетлиги *M'* ҳосил бўлади.

3. *B* томон МША дастурий таъминотидан фойдаланиб, *EKK* маромидан фойдаланилганда ҳар бир блокни алоҳида шифрлаб чиқиш блоклари кетма-кетлиги *C* ни ҳосил қилади. *SBI* маромидан фойдаланилганда ҳар бир навбатдаги блокни ундан олдинги блокни шифрлаш натижаси билан *XOR* амали асосида қўшган ҳолда шифрлаб чиқиш блоклари кетма-кетлиги *C* ни ҳосил қилади.

4. *B* томон *C* ни *I* томонга жўнатади.

5. *I* томон хэш-функция дастуридан фойдаланиб, хэш-функциянинг хэшлаш калити сифатида шифрлаш калити k ни қабул қилиб, функционал калит $k_f = h(x)$ ни ҳисоблайди. Агар жорий сеанс биринчи бўлса, унда хэш-функциянинг кириши $x=k$, акс ҳолда $x = k_{f-1}$, бу ерда k_{f-1} — олдинги сеансда ишлатилган функционал калитдир.

6. *I* томон МША дастурий таъминотидан фойдаланиб, *EKK* маромидан фойдаланилганда ҳар бир блокнинг шифрини алоҳида очиб чиқиш блоклари кетма-кетлиги *M* га мос бўлган блоклар кетма-кетлиги *M'* ни ҳосил қилади. SBI маромидан фойдаланилганда ҳар бир навбатдаги блокнинг шифрини очиш натижаси ундан олдинги блокнинг шифрини очиш натижаси билан *XOR* амали асосида қўшган ҳолда шифрини очиб чиқиш блоклари кетма-кетлиги *M* га мос бўлган блоклар кетма-кетлиги *M'* ни ҳосил қилади.

7. *I* томон блоклар кетма-кетлиги *M'* нинг сўнгги блокидан "блок охири" ишоратини топиб, ундан кейинги ҳоналардаги *01* ларни ўчиради ва блокларни конкатенациялайди ва уни иккилик саноқ тизимидан дастлабки шаклга ўгиради. Натижада дастлабки ҳужжат *M* ҳосил бўлади.

2-протокол. Икки калитли маром учун шифрлаш протоколи

Протоколни бажариш бошлангунча *B* ва *I* томонлар учун сертификатланган бир хил МША дастурий таъминотига, хэш-функция h ни ҳисоблаш дастурига, шунингдек, *I* томон *B* томон билан биргаликда махфий шифрлаш калити k га ва дастлабки функционал калит k_f га эга ҳамда *B* томонга шифрлаш учун дастлабки ҳужжат *M* берилган деб ҳисоблаймиз. Шу билан бирга, томонлар функционал калитни янгилаш тартиби ва шифрлаш мароми тўғрисида ҳам келишиб олганлар деб ҳисобланади. Бунда *B* ва *I* томонларга тегишли сертификатланган бир хил дастурий таъминот, хэш-функцияни ҳисоблаш дастури ва махфий шифрлаш калити ва дастлабки функционал калит ишончли воситачи ёки калитлар алмашиш ошкора криптотизими ёрдамида етказилиши мумкин.

1. *B* томон, агар жорий сеанс биринчи бўлса, унда функционал калит k_f сифатида дастлабки функционал калит қабул қилинади, акс ҳолда хэш-функция дастуридан фойдаланиб, хэш-функциянинг хэшлаш калити сифатида шифрлаш калити k ни қабул қилиб, жорий сеанс учун функционал калит $k_f=h(k_{f-1})$ ни ҳисоблайди. Бу ерда, k_{f-1} — олдинги сеансда ишлатилган функционал калитдир.

2. В томон шифрланадиган ҳужжат *M* ни иккилик саноқ тизимига келтириб, уни узунлиги *128* (*256*) битли $n \geq 1$ блокларга ажратади. Агар сўнгги блок *128* (*256*) битдан кам бўлса, унинг охирига "блок охири" ишоратини қўйиб, қолган бўш хоналарни *01* лардан тузилган кетма-кетлик билан тўлдиради. Бунда *0* ва *1* рақамлари галма-гал алмашиб боради. Натижада *M* га мос кириш кетма-кетлиги *M'* ҳосил бўлади.

3. *B* томон МША дастурий таъминотидан фойдаланиб, *EKK* маромидан фойдаланилганда ҳар бир блокни алоҳида шифрлаб чиқиш блоклари кетма-кетлиги *C* ни ҳосил қилади. *SBI* маромидан фойдаланилганда ҳар бир навбатдаги блокни ундан олдинги блокни шифрлаш натижаси билан *XOR* амали асосида қўшган ҳолда шифрлаб чиқиш блоклари кетма-кетлиги *C* ни ҳосил қилади.

4. *B* томон *C* ни *I* томонга жўнатади.

5. *I* томон агар жорий сеанс биринчи бўлса, унда функционал калит k_f сифатида дастлабки функционал калит қабул қилинади, акс ҳолда хэш-функция дастуридан фойдаланиб, хэш-функциянинг хэшлаш калити сифатида шифрлаш калити k ни қабул қилиб, жорий сеанс учун функционал калит $k_f=h(k_{f-1})$ ни ҳисоблайди. Бу ерда k_{f-1} — олдинги сеансда ишлатилган функционал калитдир.

6. *I* томон МША дастурий таъминотидан фойдаланиб, *EKK* маромидан фойдаланилганда ҳар бир блокни алоҳида шифрини очиб чиқиш блоклари кетма-кетлиги *M* га мос бўлган блоклар кетма-кетлиги *M'* ни ҳосил қилади. *SBI* маромидан фойдаланилганда ҳар бир навбатдаги блок шифрини очиш натижасини ундан олдинги блокнинг шифрини очиш натижаси билан *XOR* амали асосида қўшган ҳолда шифрини очиб чиқиш блоклари

кетма-кетлиги *M* га мос бўлган блоклар кетма-кетлиги *M'* ни ҳосил қилади.

7. *I* томон блоклар кетма-кетлиги *M'* нинг сўнгги блокидан "блок охири" ишоратини топиб, ундан кейинги хоналардаги *01* ларни ўчиради ва блокларни конкатенациялайди ва уни иккилик саноқ тизимидан дастлабки шаклга ўгиради. Натижада дастлабки ҳужжат *M* ҳосил бўлади.

Юқорида келтирилган протоколлар барча симметрик тизимлар сингари томонларнинг бир-бирига ишончи бўлишига асосланади.

Электрон рақамли имзо бўйича давлат стандарти O'z DSt 1092:2005 "Ахборот технологиялари. Ахборотнинг криптографик ҳимояси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари" дан фойдаланишда сеанс калитли ва сеанс калитсиз маромлар назарда тутилган. Сеанс калитсиз маромда анъанавий протоколлардан фойдаланилади. Сеанс калитли маромда давлат стандартига хос протоколлардан фойдаланилади. Бундай протоколлар мажмуи [100] да келтирилган ва таҳлил этилган.

АДАБИЁТЛАР РЎЙХАТИ

1. *Брюс Шнайер.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — Москва: ТРИУМФ, 2002. — 816 с.
2. *Нильс Фергюсон, Брюс Шнайер.* Практическая криптография. — Москва: «Диалектика», 2004 г. — 432 с.
3. *Молдовян А.А., Молдовян Н.А., Гуц Н.Д.* Криптография. Скоростные шифры. — Изд.:Лори БХВ, — Петербург, 2002.
4. Защита информации. Малый тематический выпуск ТИИЭР. — Москва, 1988. — т.76, №5. — 179 с.
5. *Баричев С.Г., Гончаров В.В., Серов Р.Е.* Основы современной криптографии. — Москва: Лори Горячая Линия, — Телеком, 2002. — 120 с.
6. *Баричев С.Г., Серов Р.Е.* Основы современной криптографии. Учебное пособие. — Москва: Лори Горячая Линия, — Телеком, 2002. — 152 с.
7. *Венбо Мао.* Современная криптография. Теория и практика. — Москва — Санкт-Петербург — Киев: Лори Вильямс, 2005. — 768 с.
8. *Молдовян Н.А., Молдовян А.А.* Введение в криптосистемы с открытым ключом. — СПб: БХВ-Петербург, 2005. — 156 с.
9. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.
10. *Хасанов П.Ф.* Модели и алгебры схем цепей и систем: Дис. на соискание доктора техн. наук. — Ташкент: ТашПИ, 1975. — с. 144—250.
11. *Хасанов П.Ф.* и др. Методы анализа цепей с ключевыми элементами. — Т. “Фан”, 1983.
12. *Хасанов П.Ф.* и др. Преобразования схем электрических и электронных цепей, — Т. “Фан”, 1978.

13. *Хасанов П.Ф.* Фигурно точечные модели и диаопределители матриц. — Т. "Укитувчи", 1975.
14. «Маълумотларни шифрлашнинг мураккаб модулли алгоритми ва дастурини ишлаб чиқиш» мавзуси бўйича бажарилган илмий тадқиқот ишининг 1—6 босқич ҳисоботлари. — ЎзААА ФТМТМ, Тошкент, 2003.
15. «Ахборотни криптографик муҳофазалаш тизими бардошлилигини баҳолашнинг замонавий усулларини тадқиқ этиш. Криптографик модулларга оид хавфсизлик талабларини ишлаб чиқиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-6-босқич ҳисоботлари. — Тошкент, ЎзААА, ФТМТМ, 2005—2006.
16. *Хасанов Х.П.* Диаматрица-устунлар ва параметрлар алгебраси // Кибернетика масалалари. — Тошкент, 2006, №173. — 93—100 б.
17. *Хасанов Х.П.* Махсус ва содда тузилмали диаматрицалар // Информатика ва энергетика муаммолари. — Тошкент, 2005, №4-5. — 71—76 б.
18. *Хасанов Х.П.* Такомиллаштирилган диаматрицалар алгебраси // Infocom.uz. — Тошкент, 2005, №9. — 68—70-бетлар.
19. *Хасанов Х.П.* Диаматрицалар алгебралари асосида симметрик ва носимметрик криптотизимлар яратиш усуллари ва алгоритмлари // Состояние и перспективы развития связи и информационных технологий Узбекистана: Доклады и тезисы междунар.конференции 11—12 мая 2005 г. — Ташкент, 2005. — С. 50—51.
20. *Хасанов Х.П.* Мавжуд криптоалгоритмларни параметрлар алгебраси асосида такомиллаштиришнинг умумий усули // Информационная безопасность в сфере связи и информатизации: Тезисы докл. респ. сем. 24 ноября 2005. — Ташкент, 2005. — С. 22—24.
21. *Хасанов Х.П.* Криптографические системы на основе односторонних функций диапреобразования // Международная научно-практическая конференция. «Актуальные проблемы

использования электронной цифровой подписи». Ташкент, 24—25 мая 2006 г. Доклады и тезисы. — Ташкент, 2006. — С. 54—59.

22. *Хасанов Х.П.* ва бошқалар. Internet, Intranet va Axborot himoyasi. Электрон дарслик // CD. Тошкент, 2000, http://elamak.freenet.uz.
23. *Хасанов П.Ф., Хасанов Х.П., Хасанов Ш.П., Хасанов С.П., Хасанов З.П., Ахмедова О.П.* Рақамли имзони шакллантириш ва аутентификациялаш усули // Ўзбекистон Давлат патент идораси томонидан берилган IAP 03070-сон патенти. Устуворлик санаси: 14.08.2002.
24. *Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х., Аҳмедова О.П.* Диаэкспоненциал криптографик коммуникация, аутентификация ва махфий калитлар генерацияси системасини яратиш усули // Ўзбекистон Давлат патент идораси томонидан берилган IAP 03416 патенти. Устуворлик санаси: 19.09.2003.
25. *Хасанов П.Ф., Хасанов Х.П.* Стойкость Государственного стандарта ЭЦП Республики Узбекистан // «Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно-практической конференции PKI Forum — 2006, Санкт-Петербург, 7—10 ноября 2006.
26. *Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Ахмедова О.П.* О государственном стандарте Республики Узбекистан на алгоритм шифрования данных // Aloqa dunyosi. — Тошкент, 2007, № 1 (7).— 57—71 бетлар.
27. *Ахмедова О.П.* Аналог схемы электронной цифровой подписи К. Шнорра в алгебре с параметром // Международная научно-практическая конференция. «Актуальные проблемы использования электронной цифровой подписи» 24—25 мая 2006 г. Доклады и тезисы. — Ташкент, 2006.— С. 64—67.

28. O‘z DSt 1105:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми».
29. O‘z DSt 1106:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси».
30. *Аҳмедова О.П.* Уч параметрли бир томонлама функциялар ва уларнинг хоссалари // ТошДТУ хабарлари. — Тошкент, 2006, №2.— 46—48 б.
31. *Аҳмедова О.П.* Усовершенствованные алгоритмы электронной цифровой подписи К. Шнорра // Кимёвий технология. Назорат ва бошқарув. — Тошкент, 2006, №4. — 83—87 б.
32. *Бабаш А.В., Шанкин Г.П.* История криптографии. Часть I. — Москва: Лори Гелиос АРВ, 2002. — 240 с.
33. *Бабаш А.В., Шанкин Г.П.* Криптография. — Москва: Лори Гелиос АРВ, 2002. — 512 с.
34. *Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х., Аҳмедова О.П.* Ахборотнинг криптографик муҳофазаси тарихи (Дастлабки ва формал криптография даври) // Aloqa dunyosi. — Тошкент, 2005. — №1 (4) — 32—37 б.
35. *Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х., Аҳмедова О.П.* Ахборотнинг криптографик муҳофазаси тарихи (Илмий криптография даври) // Aloqa dunyosi. — Тошкент, 2005, №2 (5). — 47—53 бетлар.
36. *Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Аҳмедова О.П.* Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. — Тошкент, 2006, №1 (6). — 59—74 бетлар.
37. *Шеннон К.* Теория и связи в секретных системах. Работы по теории информации и кибернетике. — М.: Иностранная лит. 1963. — 243 с.
38. «Ошкора калитли криптотизимларни криптотаҳлиллаш учун қуролу воситалар ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий тадқикот иши-

нинг 1—8 босқич ҳисоботлари. — ЎзААА ФТМТМ, Тошкент, 2003.
39. *Diffie, W., Hellman, M.E.* New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. — Pp. 644—654.
40. *Диффи У.* Первые десять лет криптографии с открытым ключом // Перевод с англ. Защита информации. Малый тематический выпуск ТИИЭР. — Москва, 1988. — т.76, №5. — С. 54—74.
41. *Диффи У., Хэллман М.Е.* Защищенность и имитостойкость: Введение в криптографию // Перевод с англ. Защита информации. Малый тематический выпуск ТИИЭР. — Москва, 1979, т. 67, №3. — С. 71—109.
42. US Patent, Hellman, et al. Cryptographic apparatus and method, 4.200.770, April 29, 1980.
43. US Patent, Hellman, et al. Exponentiation cryptographic apparatus and method, 4.424.414, January 3, 1984.
44. Hellman M. A cryptanalytic time-memore trade-off // IEEE Transactionson Information Theory, vol. IT-26, 1980. — Pp. 401—406.
45. Rivest R.L., Shamir A., Adleman L.A. Method of Obtaining Digital Signature and Publice-Key Grypto System // ACM, V.21, №2, 1978. — Pp. 120—126.
46. Rivest R. RSA chips (past/present/future) // Presented at Eurocrypt 84, Paris, France, 1984. — Pp. 9—11.
47. Rivest R.L. The RC5 Encryption Algorithm // Fast Software Encryption, Second International Workshop / Lecture Notes in Computer Science. Springer-Verlag. Vol. 1008, 1995. — Pp. 86—96.
48. US Patent, Rivest, et al. Cryptographic communications system and method, 4.405.829, September 20, 1983.
49. US Patent, R. Rivest, A. Shamir, and L. M. Adleman: Cryptographic Communications System and Method. 4. 405. 829, 1983.

50. Rivest R., Shamir A., and Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Comm. ACM, vol. 21, №2 1978. — Pp. 120—126.
51. Shamir, A. On the generation of cryptographically strong pseudo-random sequences // ACM Transactions on Computer Systems, vol. 1, 1983. — Pp. 38—44.
52. Shamir, A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem // IEEE Transactionson Information Theory, vol. IT-30, 1984. — Pp. 699—704.
53. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO'85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). — Pp. 396—402.
54. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. — Pp. 469—472.
55. US Patent, Schnorr. Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system. 4.995.082. — 1991.
56. Ong H. and Schnorr C.P. Signatures sheme based on quadratic forms // In Advances in Cryptology: Proceedings of CRYPTO 83. New York, NY: Plenum.1984. — Pp. 117—132.
57. Ong H., Schnorr C.P., and Shamir A. An efficient signature sheme based on quadratic equatins // In Proceedings of 16th ACM Symp. On Theory of Computing, 1984. — Pp. 208—216.
58. Miller V. Use of elliptic curves in cryptography // Advances in cryptology — CRYPTO'85 (Santa Barbara, Calif., 1985). 1986. (Lecture Notes in Comput. Sci.; V. 218). P. 417—426.
59. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). — Pp. 173—193.
60. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. — Pp. 203—209.
61. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы // Пер с англ. — Москва: Мир, 1988. — 320 с.

62. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography // CRC Press, 1996. — 780 pp.
63. Menezes A., Okamoto T. & Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory, 39 (1993). — Pp. 1639—1660.
64. Schneier B. Applied Cryptography // John Wiley &Sons, Inc., 1996. — 758 pp.
65. *Шнайер Б.* Слабые места криптографических систем // Открытые системы. — 1999, № 1. — С. 31—36.
66. *Василенко О.* Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.—328 с.
67. *Матюхин В.Г.* От национальной инфраструктуры открытых ключей — к трансграничному международному электронному взаимодействию // Международная научно-практическая конференция. «Актуальные проблемы использования электронной цифровой подписи» 24—25 мая 2006 г. Доклады и тезисы. Ташкент, 2006. — С. 7—10.
68. *Молдовян Н.А.* Проблематика и методы криптографии. — СПб: БХВ-Петербург, 1998. — 212 с.
69. *Ростовцев А.Г.* Алгебраические основы криптографии. — СПб: Мир и Семья, 2000. — 296 с.
70. *Ростовцев А.Г., Маховенко Е.Б.* Введение в криптографию с открытым ключом. — СПб: Мир и Семья, 2001. — 336 с.
71. *Ростовцев А.Г., Матвеев В.А.* Защита информации в компьютерных системах. Элементы криптологии. // Под редакцией П.Д. Зегжды. — СПб: ГТУ, 1993. — 365 с.
72. *Арипов М., Пудовченко Ю.* Основы криптологии. — Ташкент, 2004
73. *Арипов М., Пудовченко Ю.* Современные суперкомпьютеры и проблемы криптографической силовой атаки // Ташкент: НУУ, 2000.— 16 с.
74. *Акбаров Д.Е., Ясинский В.В.* Математика в становлении науки криптологии. К.: Политехника , 2001. 42 стр.

75. *Каримов М.М.* Организация корпоративных компьютерных сетей с интегрированной системой защиты информации. // Дис. на соискание доктора техн. наук. — Ташкент: ТашГТУ, 2003.
76. Цикл статей по криптографии Андрея Винокурова: http://www.enlight.ru/ib/tech/crypto/index.htm.
77. *Винокуров А.* Современность практической криптографии // Системы безопасности связи и телекоммуникаций. — 2003. — №10. — С. 218—221.
78. Federal Information Processing Standards Publication 46-3. U.S. Department of Commerce/National Institute of Standards and Technology. Data Encryption Standard (DES). 1999
79. ГОСТ 28147-89. Государственный Стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
80. *Стахов А.П.* «ЗОЛОТАЯ» КРИПТОГРАФИЯ, Таганрог http://www.goldenmuseum.com/ http://www.trinitas.ru/rus/
81. Немецкие ученые успешно решили проблему дискретного логарифмирования по модулю 530-битного (160 десятичных знаков) простого числа р.— http://www.securitylab.ru
82. *Алгулиев Р.М., Имамвердиев Я.Н.* Исследование международных и национальных стандартов цифровой подписи на эллиптических кривых // Вопросы защиты информации. — Москва, 2005. —№2(69) — С. 2—7.
83. Алгоритмические основы эллиптической криптографии / *Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А.* — Москва, МЭИ, 2000. — 100 с.
84. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / *Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А.* — Москва, МЭИ, 2006. — 328 с.
85. Асимметричная криптография на эллиптических кривых // Open PGP в России. — http: //. www.pgpru.com

86. Johnson D. and Vanstone S. The elliptic curve digital signature algorithm (ECDSA) // International Journal on Information Security, 1 (2001). — Pp. 36—63.
87. *Ященко В.* Криптография, раньше была засекречена // «Компьютера», 1998, №20.
88. ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
89. СТБ 1176.2-99. Государственный стандарт Республики Беларусь. Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи.
90. ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка // Научно-практический семинар. — Киев, 2003. — bezpeka.org/ru/activ.html.
91. ГОСТ Р 34.10-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
92. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
93. Federal Information Processing Standards Publication 186-2. U.S. Department of Commerce/National Institute of Standards and Technology. Digital Signature Standard (DSS). 2000.
94. *Аҳмедова О.П.* Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.
95. Алгоритм хэширования SHA-1 взломан. http://asechka.ru/archive

96. ГОСТ Р 34.11-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
97. *Костин А.А., Молдовян Д.Н., Молдовян Н.А.* Новая криптосистема с открытым ключом на основе RSA-модуля // Вопросы защиты информации, Москва — 2005, № 1.
98. Рахимова М. Алгоритмы составления таблиц схем корректирующих устройств и фильтров: Автореф. дис. канд. техн. наук. — Тошкент: ТошПИ, 1980. — 7 б.
99. *Коробейников А. Г., Гатчин Ю.А.*. Математические основы криптологии. Учебное пособие. Санкт-Петербург — 2004.
100. *Исаев Р.И.* Обеспечение устойчивости функционирования сетей и систем передачи информации методом контрольного сеансового ключа. Тез. докл. международной научно-практической конференции PKI Forum- 2007, Санкт-Петербург, 6—8 ноября 2007.
101. *Алексеев В. Б.* Сложность умножения матриц. Обзор // Кибернетич. сборн. 1988. Вып. 25. С. 189—236.

Хасанов Хислат Пўлатович

ТАКОМИЛЛАШГАН ДИАМАТРИЦАЛАР АЛГЕБРАЛАРИ ВА ПАРАМЕТРЛИ АЛГЕБРА АСОСИДА КРИПТОТИЗИМЛАР ЯРАТИШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

Муҳаррир *Ё. Аҳмедова*
Техник муҳаррир *А. Солиҳов*
Мусаҳҳиҳ *Т. Азизова*

Тошкент — «ФТМТМ» — 2008

Босишга рухсат берилди 14.05.08. Бичими 60x90$^{1}/_{16}$. Шартли б.т. 13.0.
Нашр т. 13,2. Адади 1000. 145-сонли буюртма.

«ARNAPRINT» МЧЖ босмахонасида чоп этилди.
100182, Тошкент, Ҳ.Бойқаро кўчаси, 41 уй.