ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

“Ахборот хавфсизлиги” кафедраси

Қўлёзма ҳуқуқида

Нормўминов Фурқат Қувондиқович

ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА АСОСЛАНГАН КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИНИНГ ТАҲЛИЛИ ВА ТАДҚИҚИ

Мутахассислик: 5А523504 - «Криптография ва криптотаҳлил»
магистр академик даражасини олиш учун ёзилган
Диссертация

Кафедра мудири
т.ф.н., доц. Юсупов С.Ю.
_____

Илмий раҳбар
т.ф.н. Ахмедова О.П.
_____

“_____” _____2012 й.

Тошкент – 2012

МУНДАРИЖА

Кириш..... **4**

1-БОБ КАЛИТЛАРНИ ТАҚСИМЛАШ БЎЙИЧА МАВЖУД ХАЛҚАРО АЛГОРИТМЛАРНИНГ ТАДҚИҚИ ВА ТАҲЛИЛИ..... **7**

1.1 Калитларни бошқариш масаласи..... **7**

1.2 Криптографик калитларни тақсимлаш усуллари ва схемалари..... **12**

1.3 Носимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари..... **22**

1.4 Симметрик криптотизимларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари..... **33**

1.5 Калитларни тақсимлаш алгоритмларининг қиёсий таҳлили ва таснифи..... **41**

1-боб бўйича хулосалар..... **44**

2-БОБ ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА АСОСЛАНГАН КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИ ВА ПРОТОКОЛЛАРИ..... **46**

2.1 Эллиптик эгри чизиқлар криптографияси..... **46**

2.2 Диффи –Хеллманнинг ECDH калитларни тақсимлаш алгоритми..... **51**

2.3 Эллиптик эгри чизиқли MQV калитларни тақсимлаш алгоритми..... **53**

2.4 Эллиптик эгри чизиқли Месси-Омар калитларни тақсимлаш алгоритми..... **55**

2.5 Эллиптик эгри чизиқли криптотизимлар учун Эль Гамал калитларни тақсимлаш алгоритми..... **57**

2.6 Модуль арифметикасига асосланган протоколлар..... **58**

2.7 Эллиптик эгри чизиқларга асосланган протоколларнинг криптографик бардошлилиги..... **59**

2-боб бўйича хулосалар..... **65**

3-БОБ ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА АСОСЛАНГАН КРИПТОБАРДОШЛИ КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИ ВА УЛАРНИНГ ДАСТУРИЙ **67**

ТАЪМИНОТИ.....
3.1 Эллиптик эгри чизиқли алгоритмларни параметрли кўринишга ўтказиш усули..... **67**
3.2 Параметрли Диффи-Хеллман калит алмашиш алгоритми..... **69**
3.3 Параметрли эллиптик эгри чизиққа асосланган Диффи-Хеллман калит алмашиш алгоритми..... **70**
3.4 Диффи-Хеллман калитларни тақсимлаш алгоритми асосида дастурий таъминот ишлаб чиқиш..... **73**
3.5 Эллиптик эгри чизиқли ва параметрли Диффи-Хеллман алгоритмлари асосида дастурий таъминотларни яратиш..... **76**
3.6 Параметрли алгебрага асосланган калитларни тақсимлаш алгоритмларининг қиёсий таҳлили..... **86**
3-боб бўйича хулосалар..... **90**
ХУЛОСА..... **91**
ФОЙДАЛАНИЛГАН АДАБИЁТЛАР..... **93**
Илова. Дастур коди..... **97**

КИРИШ

Диссертация ишининг долзарблиги. Бутун жаҳонда сўнгги йилларда ахборот технологияларининг жадал суръатлар билан ривожланиб бориши натижасида ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Шу боис Республикамизда бу йўналиш жадал суръатлар билан ривожланмоқда. Президентимизнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» ПҚ-614–сон қарори шулар жумласидандир [2].

Ахборот-коммуникация тизимида маълумотларни махфий ёки конфиденциал алмашув жараёни учун криптографик тизимлар яратиш билан бир қаторда шу тизимда калитлар бошқариш масаласини ишончли ҳал этиш муҳим ўрин тутади. Чунки танланган криптотизим қанчалик мураккаб ва ишончли бўлмасин, ундан амалда фойдаланиш жараёнлари калитларни бошқариш масаласи билан боғликдир [1-5]. Агар маълумотларнинг махфий алмашинуви оз сонли фойдаланувчилар билан бўлса, калитлар алмашинуви жараёнида ноқулайликлар туғилмайди. Аммо ахборот-коммуникация тизимида маълумотларнинг махфий алмашинуви юзлаб, минглаб ва ҳатто миллионлаб фойдаланувчилар билан бўлса, калитларни бошқаришнинг ўзига хос алоҳида муҳим масалалари келиб чиқади.

Мазкур диссертация иши Ўзбекистон Республикаси Президентининг ПҚ-614–сон қарори ижросини таъминлаш йўлида бажарилаётган илмий-тадқиқот ишларидан бири ҳисобланади [2]. Криптографияда калитларни тарқатиш роли доимо асосий муаммолардан бири бўлиб келган. Хорижий давлатларда бу соҳада қатор илмий изланишлар қилинган ва криптографик алгоритмлар яратилган.

Ҳозирги кунда ҳужжат алмашув тизимларида махфий шифрлаш калитларини тақсимлаш учун Диффи-Хеллман усулидан фойдаланилади ва бу усулга асосланган хорижий алгоритмлар ишлаб чиқилган [1-10]. Ўзбекистон Республикасида эса махфий шифрлаш калитларини тақсимлаш учун стандарт даражасидаги алгоритм ишлаб чиқилмаган. Ўзбекистонда ҳам бу соҳада илмий изланишлар бошлаб юборилган. Шу туфайли эллиптик эгри

чизиқлардан фойдаланишга асосланган бардошлилиги оширилган калитларини тақсимлаш алгоритмларини ишлаб чиқиш долзарб масаладир. Мазкур магистрлик диссертация иши криптографик бардошлиги юқори бўлган эллиптик эгри чизиқларга асосланган калитларни тақсимлаш алгоритмларининг таҳлили ва тадқиқига қаратилганлиги унинг долзарблилигидан далолат беради.

Диссертация ишининг мақсади. Ушбу магистрлик диссертация ишини бажаришдан кўзланган мақсад эллиптик эгри чизиқларга асосланган калитларни тақсимлаш алгоритмларининг таҳлили ва тадқиқини амалга ошириш ҳамда параметрлар алгебрасига асосланган калитлар тақсимлаш алгоритмини ишлаб чиқишдан иборат.

Диссертация ишининг вазифаси. Кўзланган мақсадни амалга ошириш учун магистрлик диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

– калитларни тақсимлаш бўйича мавжуд алгоритмлар ва протоколларни тадқиқ ва қиёсий таҳлил этиш;

– калитларни тақсимлаш алгоритмларини маълум белгилар асосида таснифлаш;

– эллиптик эгри чизиқларга асосланган калитларни тақсимлаш алгоритмларини тадқиқ ва таҳлил этиш;

– параметрли алгебра ва унга асосланган калитларни тақсимлаш криптотизимларини яратиш усулларини тадқиқ этиш;

– параметрли алгебрага асосланган калитларни тақсимлаш алгоритмини шакллантириш;

– эллиптик эгри чизиқли параметрли алгебрага асосланган криптографик бардошлиги юқори бўлган калитларни тақсимлаш алгоритмининг дастурини ишлаб чиқиш.

Диссертация ишининг объекти ва предмети. Ушбу магистрлик диссертация ишида тадқиқот объекти бўлиб калитларни тақсимлаш алгоритмлари ва протоколлари хизмат қилади.

Тадқиқот предмети сифатида эса эллиптик эгри чизиқлар ҳамда параметрли алгебра амаллари ва хоссалари хизмат қилади.

Диссертация ишининг тадқиқот усуллари. Диссертация ишида информатика ва математика асослари, сонлар назарияси, модуль

арифметикаси, Галуа майдонлари, эллиптик эгри чизиқлар назарияси ҳамда параметрли алгебрадан фойдаланилган.

Диссертация ишининг илмий янгилиги. Мазкур магистрлик диссертацияси натижасида эллиптик эгри чизиқли параметрли алгебрага асосланган криптографик бардошлиги юқори бўлган калитларни тақсимлаш алгоритми ва унинг дастурини ишлаб чиқилди ҳамда унинг криптографик бардошлиги баҳоланди.

Диссертация ишининг амалий аҳамияти. Ушбу магистрлик диссертацияси ишида ишлаб чиқилган алгоритмлардан миллий электрон ҳужжат айланиш тизимларида фойдаланиш уларнинг муҳофазасини оширишга хизмат қилади.

Диссертация ишининг тузилмаси ва ҳажми.

Ушбу диссертация иши кириш қисми, 3 та бўлим, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат.

1-БОБ. КАЛИТЛАРНИ ТАҚСИМЛАШ БЎЙИЧА МАВЖУД ХАЛҚАРО АЛГОРИТМЛАРНИНГ ТАДҚИҚИ ВА ТАҲЛИЛИ

1.1. Калитларни бошқариш масаласи

Ҳозирги кунда криптографик тизимлар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири бўлиб, электрон ҳужжат айланиш ва электрон тўлов тизимларида электрон рақамли имзо шакллантириш ва аутентификация масалаларини ечиш учун фойдаланилади [8-11]. Криптографик тизимларда асосий тушунчалардан бири калит тушунчаси ҳисобланади. Криптографик калитлар носимметрик криптотизимлар учун очиқ ва махфий калитларнинг умумий номи бўлиб, электрон рақамли имзони ҳисоблаш ёки текшириш, шунингдек шифрлаш ва дастлабки матнга ўгириш учун қўлланиладиган символлар кетма-кетлигини ифодалайди. Криптографик алмаштиришларни амалга оширувчи шахсгагина тегишли ва маълум бўлган калит махфий калит деб аталади [12].

Калитлар ҳақидаги маълумот деганда, ахборот-коммуникация криптотизимида мавжуд бўлган барча калитлар тўплами ва уларнинг муҳофазаси билан боғлиқ маълумотлар тушунилади. Агарда калитлар ҳақидаги маълумотларни етарли даражадаги ишончли муҳофазали бошқаруви таъминланмаса, табиийки, рақиб томонга ахборот-коммуникация тизимидаги деярли ихтиёрий маълумотни олиш учун тўла имконият туғилади. Калитларни бошқариш криптографик калитлар ва хавфсизлик билан боғлиқ бошқа параметрлар (масалан, инициализациялаш векторлари ва пароллар)ни бошқаришни, шунингдек, уларни генерация қилиш, сақлаш, ўрнатиш, киритиш, чиқариш ва ноллашни ўз ичига оладиган калитлар ҳаётининг тўлиқ цикли давомида бажариладиган амалларни ўз ичига олади.

Криптографик калитларни бошқариш соҳасида асосий халқаро стандарт сифатида 3 қисмдан иборат ISO/IEC 11770 стандартидан фойдаланилади [39-41].

Калитларни бошқариш жараёни қуйидаги учта муҳим бўлган жараёнларга аҳамият беришни талаб этади:

- калитлар генерацияси;
- калитларнинг тўпланиши;
- калитларларнинг тақсимланиши.

Калитларни осон эслаб қолиш мақсадида тасодифий танланмаган калитлардан фойдаланиш хавфсизликни таъминлай олмайди. Ахборот-коммуникация тизимларида тасофий калитларни генерациялашнинг махсус аппарат ва дастурий усулларидан фойдаланилади.

Калитларнинг тўпланиши деганда, уларни сақлаш, ҳисобга олиш ва йўқотишни ташкиллаштириш тушунилади. Калит бузғунчи учун ўзига энг жалб этувчи объект ҳисобланиб, унга конфиденциал ахборот учун йўл очади, шунинг учун ҳам калитлар тўпламига катта аҳамият бериш талаб этилади. Махфий калитлар ҳеч қачон ошкора ҳолда ахборот ташувчиларга ёзилмаслиги, яъни уни ўқиб ва кўчириб бўлмаслик керак. Етарли даражада мураккаб ахборот-коммуникация тизимларида битта фойдаланувчи катта ҳажмдаги калит ахборотлар билан ишлаши мумкин ва баъзида эса калит ахборотлар бўйича кичик маълумотлар базаси ташкил этиш зарурияти пайдо бўлади. Бундай маълумотлар базаси фойдаланилган калитларни қабул қилишга, сақлашга, ҳисобга олишга ва йўқотишга жавобгар ҳисобланади. Шундай қилиб ишлатилган калитлар ҳақидаги барча ахборотлар шифрланган ҳолда сақланиши керак. Ахборот тизимларидаги калит ахборотларни мунтазам равишда янгилаб туриш ахборот хавфсизлигининг муҳим шарти ҳисобланади.

Симметрик криптотизимлардан муваффақиятли фойдаланиш учун махфий калит тўғрисида келишиб олиш, яъни турли фойдаланувчилар ўртасида калитлар тақсимланган бўлиши керак. Тақсимланган калитларга тақсимлашнинг тезкорлиги ва аниқлиги, тақсимланадиган калитларнинг махфийлиги каби талаблар қўйилади [3-5].

Статик (узоқ вақтли) калит. Узоқ вақт давомида ишлатиладиган калит статик калит дейилади. “узоқ” сўзининг маъноси калитнинг қаерда ва қанча вақт давомида (бир неча соатдан бир неча йилгача) ишлатилишга боғлиқ. Статик калитни очилиши одатда асосий муаммонинг ҳалокатли оқибати ҳисобланади.

Сеанс (қисқа муддатли) калитидан қисқа вақт (бир неча сониядан бир кунгача) оралиғида фойдаланилади. Одатда ундан бир мартали алоқада махфийликни таъминлаш учун фойдаланилади. Сеанс калитининг очилиши фақат сеанснинг махфийлигини бузилишига олиб келади, лекин бу бутун криптотизимнинг криптобардошлилигига ҳеч қандай таъсир кўрсатмаслиги керак.

Калит тақсимоти - криптографиянинг асосий масалаларидан бири бўлиб, унинг бир қанча ечимлари мавжуд, улардан моси вазиятга боғлиқ ҳолда танланади [3-5].

Физик тақсимот. Ишончли курьерлар ёки қуролланган соқчилар ёрдамида калитлар анъанавий физик усул билан юборилиши мумкин. XX асрнинг етмишинчи йилларига қадар тармоқ ўрнатишда бу ҳақиқатан ҳам калит тақсимотининг ягона хавфсиз усули эди. Бунинг ўзига хос қийинчиликлари ҳам мавжуд бўлиб, улардан энг асосийси криптотизимларнинг криптобардошлилиги фақат калитга боғлиқ бўлмай, курьерга ҳам боғлиқ бўлади. Агар курьерни сотиб олиш, ўғирлаш ёки ўлдириш мумкинлиги эътиборга олинса, у ҳолда тизим обрўсизланиши мумкин.

Махфий калитли протоколлар ёрдамида тақсимлаш. Агар узоқ муддатли махфий калитлар фойдаланувчилар ва бирор ишонч маркази орасида тақсимланган бўлса, у ҳолда ундан калитларни генерация қилишда ва ихтиёрий иккита фойдаланувчи орасида алмашинув зарурати туғилганда фойдаланилади.

Носимметрик калитли протоколлар ёрдамида тақсимлаш. Носимметрик (очиқ) калитли криптотизимлардан фойдаланувчи шериклар воситачига ишонмаса ва учрашиш имконига эга бўлмасалар, калит тақсимлаш протоколига мувофиқ онлайн режимида умумий махфий калит тўғрисида келишиб олишлари мумкин. Бу очиқ калитли шифрлаш техникасининг энг кўп тарқалган иловасидир. Катта ҳажмдаги маълумотни очиқ калит ёрдамида бевосита шифрлаш ўрнига томонлар олдиндан махфий калитни келишиб олишади. Кейин аниқ маълумотларни шифрлаш учун келишилган калит билан симметрик шифр қўлланилади.

Муаммонинг кўламини тушунтириш учун ўзаро бир-бирлари билан махфий ахборот алмашинувчи n та иштирокчига хизмат кўрсатиш учун $\frac{n(n-1)}{2}$ та турли махфий калит керак бўлади. n ошиши билан катта миқдордаги калитларни бошқариш муаммоси пайдо бўлади. Масалан, 20 000 талаба бўлган университетга 199 миллиондан кўп алоҳида махфий калитлар керак бўлади [3-4]. Катта миқдордаги махфий калитларнинг ҳосил қилиниши уларнинг бошқарувида катта муаммоларни келтириб чиқаради.

Бундай муаммонинг ечимларидан бири шундаки, ҳар бир иштирокчига фақат битта калит бириктириб қўйилади ва бу калитдан фойдаланиб у ИМ (ИМ) билан боғланади. Бу ҳолда n фойдаланувчили тизим n та калит талаб этади. Агар икки иштирокчи махфий ахборот алмашмоқчи бўлса, улар фақат шу ахборотни узатишда қўллаш учун калит генерация қилишади. Бу калитни сеанс калити деб аталади.

Махфий калит тўла маънода тасодифий бўлиши керак, чунки бузғунчи аввалдан калит ва хабарларнинг тақсимланиш эҳтимоллигини билса, калит ҳақида ҳам маълумотга эга бўлиши мумкин. Барча калитлар бир хил эҳтимолликка эга бўлиши ва тасодифий сонларнинг ҳақиқий генератори ёрдамида ҳосил қилиниши керак. Лекин бутунлай тасодифий сонлар манбаини яратиш жуда ҳам қийин. Бундан ташқари ҳақиқий тасодифий калит амалиёт учун қулай бўлгани билан уни инсон миясида сақлаб туриш мураккаб. Шунинг учун кўпгина тизимлар махфий калитни генерация қилишда парол ёки мос иборалардан фойдаланади. *PIN* – кодга ўхшайдиган парол, яъни 0 дан 9999 оралиғида ётувчи оддий сонни тўғридан-тўғри ҳужум билан осон топиш мумкин. 8 хонали сонлардан иборат паролдан фойдаланиш ҳам бизга етарли хавфсизликни таъминламайди.

Калитларни танлашда 20-30 символли узун иборалардан фойдаланиш мумкин, бироқ бу ҳам ечим бўлмайди, сабаби табиий тилдаги ҳарфлар кетма-кетлиги бутунлай тасодифий эмас.

Исмларга ёки ибораларга асосланган қисқа пароллар кўплаб катта корхоналарнинг умумий муаммосидир. Улардан кўпчилига паролда

– ҳеч бўлмаганда битта бош ҳарф иштирок этишини;

– ҳеч бўлмаганда битта катта ҳарф иштирок этишини;

– ҳеч бўлмаганда битта рақам иштирок этишини;

– ҳеч бўлмаганда битта рақам ва ҳарфдан бошқа белги иштирок этишини;

– паролнинг узунлиги 8 символдан кам бўлмаслигини талаб этишади.

Лекин келтирилган қоидалар луғат бўйича ҳужумдан ташқари саккизта символни ҳақиқатан тасодифий танлагандаги мумкин бўлагн максимал пароллар сонини таъминламайди.

Калитларни генерациялаганда ва сақлаганда калитларнинг яроқлилик муддатига аҳамият бериш керак. Фойдаланилаётган калит қанча кўп муомалада бўлса, бузғунчига уни очиш шунчалик осон бўлади ва у шунчалар катта қийматга эга бўлади. Бу асосий қоида бўлиб калитнинг яроқлилик муддати тугаши билан уни тўғри йўқотиш керак. Муаммони “del” ёки “rem” командаси орқали операцион тизим зиммасига юклаш бузғунчининг қаттиқ дискдаги ахборотни қайта тиклай олмаслигини кафолатламайди. Чунки файлни йўқотишда унинг ичидаги нарсалар йўқолмайди, балки тизимга фақат хотиранинг унга ажратилган ячейкалари энди бошқа янги маълумотларни ёзиш учун бўшлигини билдиради.

Асосий муаммолардан бири махфий калит тақсимотининг хавфсиз бошқарувидир. ИМ ишлатилганда ҳам унинг ҳар бир иштирокчиси учун қандайдир калит олиш усули керак бўлади.

Бу муаммони ечиш йўлларидан бири калитни парчалаш (ёки махфийликни бўлиш) бўлиб, бунда калит бир неча бўлакларга бўлинади [3-4, 6]:

$$k = k_1 \oplus k_2 \oplus \ldots \oplus k_r .$$

Унинг ҳар бир қисми ўзининг канали бўйича юборилади. Калитни аниқлаши учун бузғунчи барча каналларга бир вақтда уланиши керак бўлади. Бунда агар бузғунчи калит қисми узатиладиган каналлардан бирига киришга муваффақ бўлса, у калитнинг қонуний тикланишига тўсқинлик қилиши мумкин.

Юқорида айтиб ўтилгандек, n та иштирокчи ўзаро бир-бирлари билан махфий ахборот алмашиниши учун $\frac{n(n-1)}{2}$ та узоқ муддатли турли махфий калит керак бўлади. Таъкидлаб ўтилганидек, бу ўз навбатида катта миқдордаги калитларни бошқариш ва уларни тақсимлаш муаммосини келтириб чиқаради. Аввал айтилгандек бунда сеанс калитларидан ва бир нечта статик калитлардан фойдаланиш афзалроқ.

Бу масалани ечиш учун кўплаб протоколлар ишлаб чиқилган, уларда сеанс калитини тақсимоти учун симметрик калитли криптографиядан фойдаланилади.

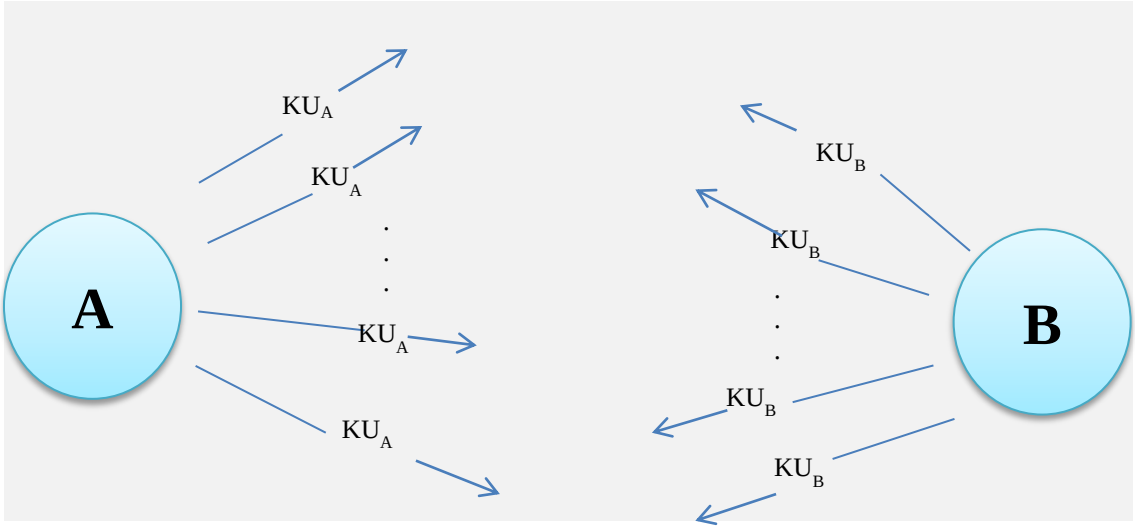
1.2. Криптографик калитларни тақсимлаш усуллари ва схемалари

Калит тақсимлаш криптографиянинг асосий масалаларидан бири ҳисобланиб, калит тақсимлаш қандай вазиятда амалга оширилаётганига қараб уни ечишнинг бир қанча усуллари мавжуд [5-7]. Бугунги кунда калитларни тақсимлашда бир қанча усуллардан фойдаланилади, бу усулларни қуйидаги синфларга жамлаш мумкин:

1. Ошкора эълон қилиш.
2. Ошкора фойдаланиш мумкин бўлган каталог.
3. Очиқ калитларнинг ИМ.
4. Очиқ калитлар сертификатлари.

Очиқ калитларни ошкора эълон қилиш

Маълумот алмашинувида иштирок этувчи ихтиёрий томон ўзининг очиқ калитини коммуникация воситалари орқали барча иштирокчиларга тақдим этиши мумкин. Бундай ёндашувнинг қулай бўлиши билан бирга, заиф томони ҳам мавжуд: ихтиёрий киши бундай ошкора эълонни бериши мумкин. Яъни, ихтиёрий киши (бузғунчи) ўзини **А** иштирокчи деб таништириб, очиқ калитини тармоқдаги бошқа иштирокчига юбориши мумкин ёки очиқ калитини барчанинг фойдаланиши учун тақдим этиши мумкин. Фирибгарлиги очилгунга қадар бузғунчи **А** иштирокчига келган барча шифр матнларни ўқиш ва очиқ калит ёрдамида аутентификациялаш (текшириш ва ҳақийқийлигини тасдиқлаш) имконига эга бўлади (1-расм).



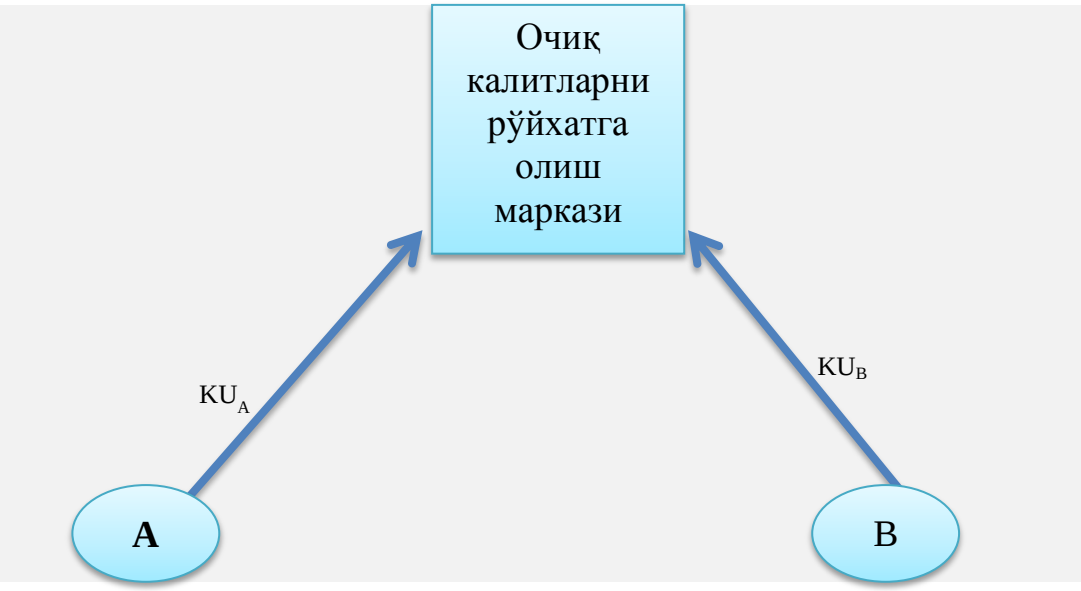
1-расм. Очиқ калитларни ошкора эълон қилиш

Ошкора фойдаланиш мумкин бўлган каталог

Очиқ калитларнинг ошкора фойдаланиш мумкин бўлган бирор динамик каталогини яратиш, ҳимояланиш даражасини нисбатан ошишини таъминлаши мумкин. Очиқ калитларнинг ошкора фойдаланиш мумкин бўлган динамик каталогини кузатиш ва тарқатиш жавобгарлиги бирор бир ишончли марказ ёки ташкилот зиммасида бўлиши лозим.

Бу жараён қуйидаги босқичларни ўз ичига олади [38]:

- ваколатланган ташкилот ҳар бир иштирокчининг исми ва очиқ калити қайд этилган каталогни шакллантиради;
- ҳар бир иштирокчи ўзининг очиқ калитини ваколатланган ташкилот ёрдамида рўйхатдан ўтказади. Бундай рўйхатдан ўтказиш иштирокчининг шахсан келишини ёки ҳимояланган коммуникация каналлари орқали бажарилишини талаб этади;
- ҳар бир иштирокчи очиқ калитдан катта ҳажмдаги маълумотни юбориш учун фойдалангани учун ёки калитнинг обрўси тушгани боис ихтиёрий вақтда мавжуд калитни бошқа янгиси билан алмаштириши мумкин;
- вақти-вақти билан ваколатланган ташкилот каталогни тўлалигича ёки унга қўшимчаларни эълон қилиб боради;
- иштирокчилар шунингдек каталогнинг электрон кўринишига кириш ҳуқуқига ҳам эга бўлиши мумкин. Бунинг учун маълумот алмашувчи иштирокчилар ва ваколатланган ташкилот орасида аутентификация воситалари қўлланилган алоқа канали талаб қилинади (2-расм).



2-расм. Ошкора фойдаланиш мумкин бўлган каталог

Бу схема якка тартибда ошкора эълон қилишга нисбатан анча ҳимояланган бўлсада, унинг ҳам заиф томонлари мавжуд. Агар бузғунчи ваколатланган ташкилотнинг махфий калитини олишга ёки ҳисоблаб топишга муваффақ бўлса, у қатъий ишонч билан сохталаштирилган очиқ калитни бериши, демакки, маълумот алмашинувида ихтиёрий иштирокчи номидан иштирок этиши ва ихтиёрий иштирокчига мўлжалланган маълумотни ўқиши мумкин бўлади. Каталогда сақланувчи қайдларни ўзгартириш ёрдамида ҳам бузғунчи шундай натижага эришиши мумкин.

Очиқ калитларнинг ишончли манбаи

Бу схемада маълумотлар алмашинувида қатнашувчи барча иштирокчилар очиқ калитларининг динамик каталогини таъминловчи бирор бош ваколатланган объект борлигини фараз қилади. Бундан ташқари ҳар бир иштирокчига марказнинг очиқ калити маълум, лекин фақатгина марказ унга мос махфий калитни билади. Бунда қуйидагилар бажарилади (3-расм):

1. **А** бошлаб берувчи сана/ВБ (вақт белгиси) қўйилган хабарни очиқ калитларнинг ИМга **В** иштирокчининг жорий очиқ калити сўровномаси билан юборади.
2. ИМ ўз махфий калити ёрдамида шифрланган хабар билан жавоб беради. Бу хабарнинг шифрини **А** бошлаб берувчи ИМнинг очиқ калитидан фойдаланиб очиши мумкин.

Бу хабар қуйидагиларни ўз ичига олиши лозим:

– **А** иштирокчи **В** иштирокчига юборадиган хабарларни шифрлаши учун В иштирокчининг очиқ калитини;

– **А** томонга жавобни аввалги юборилган сўровнома билан таққослаши ва ИМга юборилганда йўлда ўзгартириб қўйилмаганига ишонч ҳосил қилиши учун ўзига хос сўровномани;

– махсус сана/ВБни, **А** иштирокчи хабар ИМнинг **В** иштирокчини жорий калитидан фарқ қилувчи калитли эски хабарлардан бири эмаслигига инонмоғи учун;

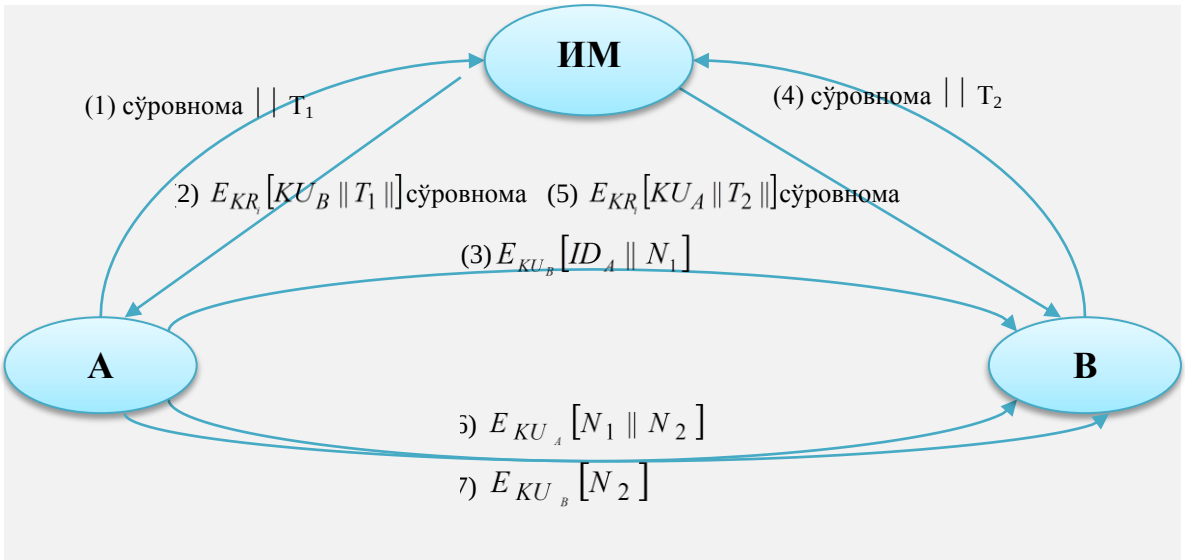
3. **А** бошлаб берувчи **В** иштирокчининг очиқ калитини сақлаб қўяди ва ундан В иштирокчига юбориладиган хабарларни шифрлашда

фойдаланади, бу хабарда **А** иштирокчининг идентификатори ва ушбу хабарнинг махсус белгиси бўлган сана ҳам қайд этилади;

4. **В** жавоб йўлловчи **А** иштирокчининг очиқ калитини ИМдан А юборувчи В қабул қилувчининг очиқ калитини олган усул билан олади;

5. **В** жавоб йўлловчи **А** бошлаб берувчига **В** нинг калити билан шифрланган хабарни ва **А** юборувчининг қўйган санасини, шунингдек қабул қилинган маълумотнинг юборувчиси **В** эканлигига ишонтириш учун, В иштирокчи томонидан генерацияланган янги санани ҳам қўшиб юборади;

6. **А** бошлаб берувчи, **В** иштирокчини жавоб юборувчи **А** иштирокчи эканлигига ишониши учун, унинг очиқ калити билан шифрланган санани қайтариб юборади.



3-расм. Очиқ калитларнинг ИМ

Шундай қилиб, олтита хабар юбориш талаб қилинар экан, лекин бошидаги тўрттасини юбориш кўпинча талаб қилинмайди, чунки иккала томон ҳам бир-бирининг очиқ калитини кейинчалик фойдаланиш учун сақлаб қўйиши мумкин, буни кешлаш дейилади. Вақти-вақти билан иштирокчи кафолатланган хавфсиз маълумот алмашиниш имкониятига эга бўлиши учун ўз адресатларининг янги очиқ калит нусхаларини сўраши лозим. Очиқ калитнинг ИМ тармоқнинг чекланган қисми бўлиб, иштирокчи унга ёзишма олиб бормоқчи бўлган ҳар бир янги адресатнинг очиқ калитини олиш учун мурожаат қилиши лозим. ИМ томонидан юритилувчи исмлар ва очиқ калитлар каталоги рухсатсиз киришга нисбатан заиф бўлиб қолади.

Очиқ калитлар сертификатлари

Сертификатлар иштирокчилар томонидан очиқ калитларнинг ИМ билан алоқасиз калит алмашинуви учун ишлатилиши мумкин бўлиб, алмашинув усули худди очиқ калитларнинг ИМнинг ўзидан олиш усулидек ишончли усулни таъминлаши зарур. Ҳар бир сертификат очиқ калит ва бошқа маълумотни ўз ичига олган бўлиб, сертификатларнинг ИМ томонидан ишлаб чиқилади ва иштирокчига мос махфий калити билан бирга берилади. Бир иштирокчи ўзининг калити тўғрисидаги маълумотни бошқа иштирокчига ўзининг сертификатини бериш орқали етказади. Бошқа иштирокчилар эса сертификат ИМ томонидан берилганлигини текширишлари мумкин. Келтирилган схемага қуйидаги талаблар қўйилади [38-39]:

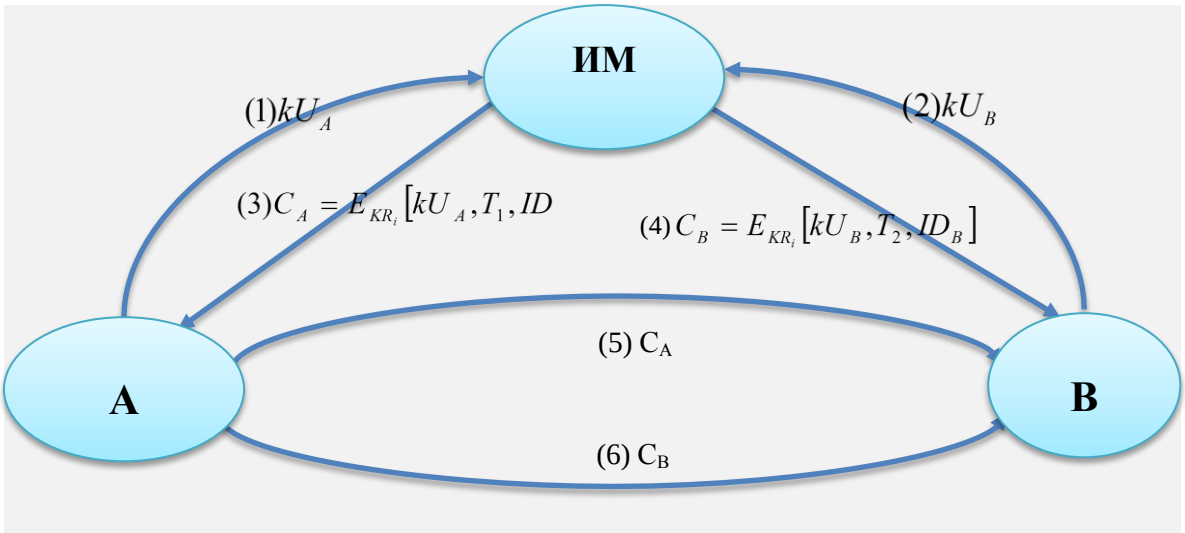
- ҳар бир иштирокчи сертификат эгасининг исми ва очиқ калитини аниқлаши учун сертификатни ўқиш имкониятига эга бўлиши керак;
- ҳар бир иштирокчи сертификат сертификатларнинг ИМ томонидан берилганлигига ва у сохта эмаслигини текшириш имкониятига эга бўлиши керак;
- фақатгина сертификатларнинг ИМгина сертификатларни яратиш ва ўзгартириш имкониятига эга бўлиши керак.

Сертификатни ишлатилиш схемаси қуйидагича (4-расм). Ҳар бир иштирокчи сертификатларнинг ИМга очиқ калитни тақдим этган ҳолда ўзига сертификат сўраб мурожаат қилади. Сўровнома шахсан ёки бирор ҳимояланган алоқа воситаси орқали мурожаат қилишни талаб этади. **А** иштирокчи учун ишонч манбаи $C_A = E_{KR_{им}}[T, ID_A, KU_B]$ сертификат беради,

бунда $kR_{им}$ – ИМнинг махфий калити; kU_B – **В** иштирокчининг очиқ калити; ID_A – **А** иштирокчининг идентификатори; T – юборилган сана/вақт. **А** иштирокчи бу сертификатни ихтиёрий бошқа иштирокчига ўқиши ва қабул қилиши учун юбориши мумкин:

$$D_{kU_{й}}[C_A] = D_{kU_{й}}\left[E_{kR_{й}}[T, ID_A, kU_A]\right] = (T, ID_A, kU_A),$$

бунда, $kU_{им}$ – ИМнинг очиқ калити; kU_A – **А** иштирокчининг очиқ калити.



4-расм. Очиқ калитлар сертификатлари

Сертификатни сертификатлар ИМнинг очиқ калити билан ўқиш мумкинлиги, сертификат айнан сертификатлар ИМдан келганлигини кафолатлайди. ID_A, kU_A элементлар олувчига сертификат эгасининг исми ва очиқ калитини билдиради. Сана/ВБ T сертификатнинг қўлланилиш муддатини аниқлайди. Сана/ВБ қуйидаги таъсирлар кетма-кетлигидан муҳофазаланган бўлиши керак. Бузғунчи **А** иштирокчининг махфий калитини билиб олган бўлсин. У ҳолда **А** иштирокчи янги (махфий ва очиқ) калитлар жуфтини генерациялайди ва сертификатларнинг ИМга янги сертификат олиш учун мурожаат қилади. Бу вақтда бузғунчи эски сертификат асосида хабар ишлаб, уни **В** иштирокчига юборади. Агар **В** иштирокчи хабарни эски очилган калит билан шифрласа, бузғунчи бу хабарни ўқий олади. Бунда вазият мумкин бўлган тизимларни эски тизим бекор қилингани тўғрисида хабардор қилинмагунча қалтислигича қолади.

Очиқ калитлар тақсимлангандан кейин хабарларни қўлга киритиш ва бузишдан ҳимояланган алоқани ташкил этиш мумкин бўлади. Лекин очиқ калитли шифрлашни қўлланилганда маълумотларни узатиш тезлиги нисбатан секинлашади, бу кўпинча иштирокчилар учун тўғри келмайди. Шунинг учун асосан Меркель томонидан таклиф этилган махфий калитларнинг тақсимлаш схемасидан фойдаланилади [38-39].

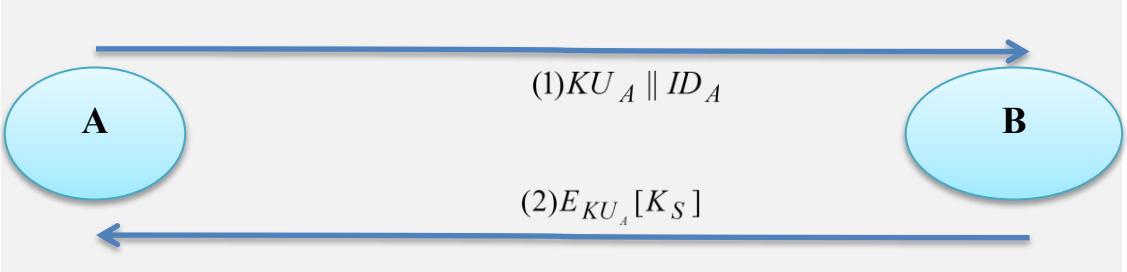
Таклиф этилган схема қуйидагидан иборат (5-расм). Агар **А** бошлаб берувчи **В** иштирокчи билан маълумот алмашмоқчи бўлса, қуйидаги жараён таклиф этилади:

1. **A** иштирокчи (очиқ/махфий) калитлар жуфтини генерациялайди ва **B** иштирокчига kU_A ва **A** иштирокчининг идентификатори бўлган ID_A ни ўз ичига олган хабарни юборади.

2. Қабул қилувчи **B** махфий калит k ни генерациялайди ва бу калитни **A** иштирокчининг очиқ калити билан шифрлаб, **A** иштирокчига юборади.

3. **A** иштирокчи $D_{kU_A}\left[E_{kU_A}\left[k_S\right]\right]$ ни махфий калитни тиклаш учун ҳисоблайди. Фақатгина **A** иштирокчи бу хабарнинг шифрини очиши мумкин бўлгани сабабли фақат шу икки иштирокчи **A** ва **B** k_A нинг қийматни билади.

4. **A** иштирокчи kR_A калитни, **B** иштирокчи эса kU_A ни йўқ қилади.



5-расм. Махфий калитлар тақсимлашнинг Меркель схемаси

Иккала **A** ва **B** иштирокчи k_A сеанс калитини қўллаб анъанавий шифрлаш ёрдамида ҳимояланган алоқадан фойдаланиши мумкин. Маълумот алмашинуви сўнгида **A** иштирокчи ҳам, **B** иштирокчи ҳам k_A ни йўқ қилади. Содда тузилишига қарамай, бу протокол эътиборга лойиқ. Алоқа бошлангунга қадар ҳам, алоқа тугагандан сўнг ҳам, ҳеч қандай калит мавжуд бўлмайди. Шунинг учун калитнинг компроментацияланиш (обрўсизланиш) хавфи жуда кичик ва бу вақтда алоқа ҳимояланган бўлади. Лекин бу протокол фаол ҳужумга нисбатан заиф. Агар **E** бузғунчининг алоқа каналига суқилиб кириш имконияти мавжуд бўлса, у аниқлангунга қадар алоқага қуйидагича путур етказиши мумкин:

1. **A** иштирокчи бир жуфт очиқ/махфий (kU_A, kR_A) калитларни генерациялайди, сўнгра kU_A ни ва **A** иштирокчининг идентификатори ID_A мавжуд бўлган хабарни **B** иштирокчига юборади.

2. **E** бузғунчи хабарни тутиб қолади, ўзининг хусусий бир жуфт очиқ/махфий (kU_E, kR_E) калитларини ҳосил қилади ва kU_E, ID_A мавжуд бўлган хабарни **B** иштирокчига юборади.

3. **B** иштирокчи k_s махфий калитни генерация қилади ва $E_{kU_A}[k_S]$ ни юборади.

4. **E** бузғунчи хабарни тутиб қолади ва $D_{kU_E}[E_{kU_E}[k_S]]$ ҳисоблаш ёрдамида k_s нинг қийматини топади.

5. Бузғунчи **A** иштирокчига $E_{kU_A}[k_S]$ ни юборади.

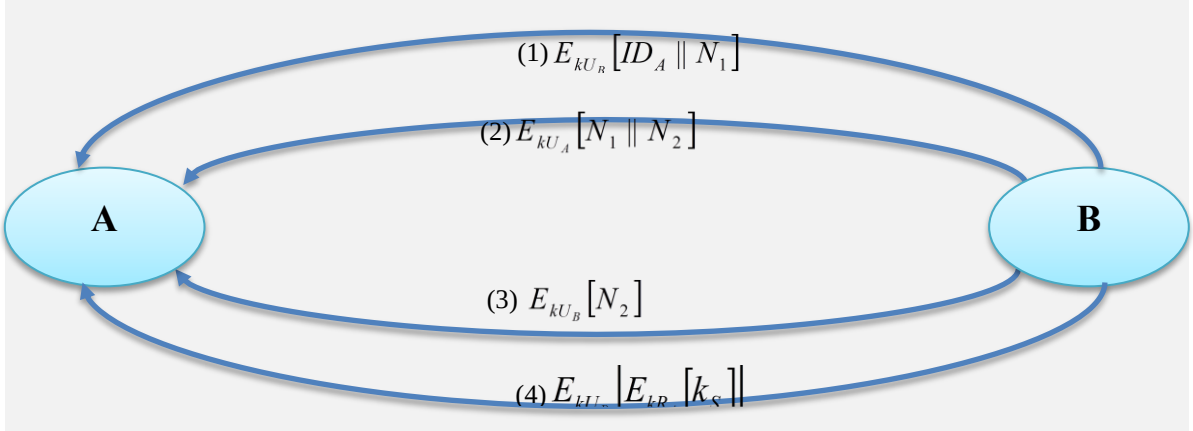
A иштирокчи ҳам **B** иштирокчига ҳам k_s маълум бўлади, лекин улар **E** бузғунчига ҳам k_s маълумлигини билишмайди. Шунинг учун **A** ва **B** иштирокчилар k_s дан фойдаланиб хабар алмашинишлари мумкин. **E** бузғунчи алоқа каналида бошқа фаол суқилиб кирмайди, фақатгина хабарларни тутиб қолади. k_s ни билган ҳолда бузғунчи ихтиёрий хабарни шифрини очиши мумкин, аммо **A** ва **B** иштирокчилар бу муаммодан бехабар бўлишади. Демак, бу протокол фақатгина хабарларни пассив тутиб қолиш мумкин бўлганида фойда беради.

Ҳозирги кунда криптографик калитларни тақсимлашнинг бир нечта схемалари мавжуд. Қуйида уларнинг баъзиларини кўриб чиқилади.

Дастлабки калит тарқатиш схемалари иккита алгоритмдан ташкил топган: бошланғич калитга оид ахборотни тақсимлаш ва калитни шакллантириш. Биринчи алгоритм ёрдамида калитга оид ахборотнинг очиқ қисми ва махфий қисми (ҳар бир томон учун) генерация қилинади, очиқ калит ҳамма кириши мумкин бўлган очиқ серверга жойлаштирилади. Иккинчи алгоритм абонентларда мавжуд бўлган махфий ва бошланғич калит маълумотининг умумий очиқ қисми ёрдамида, улар орасидаги ўзаро боғланишни амалдаги калитини ҳисоблаш учун мўлжалланган. Сақланадиган ва тақсимланадиган махфий калитли ахборотнинг ҳажмини камайтириш учун қўлланилади. Дастлабки калит тақсимлаш схемаси турғун бўлиши, яъни компроментацияда, фирибгарликда ёки баъзи абонентларнинг махфий келишувида калитнинг бир қисмини очилишини эътиборга олиниши ва тез мослашувчан – яъни обрўсизлантирилган калитларни чиқариб ташлаш орқали тезликда тиклаш ва янги абонентларни улаши имкониятини бериши керак.

Махфий калитларни конфиденциаллигини ва аутентификациясини таъминлаб тақсимлаш схемаси

Қуйидаги 6-расмда келтирилган схема фаол ва пассив ҳужумлардан ҳимояни таъминлайди.



6-расм. Фаол ва пассив ҳужумлардан ҳимояни таъминлаш схемаси

A ва **B** юқорида келтирилган схемалардан бири ёрдамида очиқ калитларини алмашинишган бўлсин. Бунда қуйидаги амаллар бажарилади:

1. **A** иштирокчи **B** иштирокчига шифрланган ахборот жўнатиш учун **A** иштирокчининг ID_A идентификаторини ва N_1 псевдотасодифий сонни ўз ичига олган хабарни **B** нинг очиқ калити kU_B ёрдамида шифрланб **B** иштирокчига юборади.

2. **B** иштирокчи **A** иштирокчига ундан олинган N_1 псевдотасодифий сонни ва янги **B** иштирокчи томонидан генерацияланган N_2 псевдотасодифий сонни ўз ичига олган, ҳамда kU_A ёрдамида шифрланган хабарни жўнатади. N_1 нинг хабарда мавжудлиги **A** иштирокчини хабар юборувчи **B** иштирокчи эканлигига ишонтиради.

3. **A** иштирокчи хабарни **B** иштирокчининг очиқ калити билан шифрлаб N_2 ни қайтариши хабар юборувчи **A** эканлигига **B** ни ишонтиради.

4. **A** иштирокчи k_S махфий калитни танлаб **B** иштирокчига $M = E_{kU_B}\left[E_{kR_A}[k_S]\right]$ хабарни юборади. **B** иштирокчининг очиқ калити билан шифрланган матнни фақатгина **B** иштирокчигина ўқий олишини, **A** иштирокчи хабарини махфий калити билан шифрлаши эса хабарни фақатгина **A** иштирокчи юборганини кафолатлайди.

5. **B** иштирокчи эса $D_{kU_A}\lfloor E_{kU_B}[M]\rfloor$ ни ҳисоблаб махфий калитни тиклайди.

Бу схеманинг бошидаги учта амал ИМдаги очиқ калит тарқатишининг учта сўнгги амалига мос келади. Натижада, махфий калитлар алмашинишда бу схема конфиденциаллик ва аутентификацияни кафолатлайди.

Гибрид схема

Махфий калит тарқатишидаги очиқ калит билан шифрлашнинг яна бир схемаси гибрид ёндашуви бўлиб, у IBM фирмасининг супер компьютерларида қўлланилади [39-40]. Бу схема калит тарқатиш маркази иштирокини кўзда тутади. Бундай уч босқичли ёндашувнинг асосида қуйидаги мантиқ ётади:

– *процедураларнинг бажарилиш тезлиги*. Бу мантиққа транзакцияларни узатишга ихтисослашган иловалар (приложение) мосланган бўлиб, бунда сеанс калитлари тез-тез алмаштириб турилиши лозим. Сеанс калитларини ошкора калитли схема ёрдамида тарқатилиши, бу схемада шифрлаш ва шифрни очиш жараёнида ишлатиладиган ҳисоблаш ресурсларига қўйиладиган катта талаблар ҳисобига тизимнинг унумдорлигини жуда ҳам пасайтириб юбориши мумкин эди. Уч босқичли иерархияда очиқ калит билан шифрлаш иштирокчилар билан калит тарқатувчи марказ орасида тақсимланувчи асосий калитни ўзгартириш каби баъзи ҳоллардагина ишлатилади;

– *қайтарилувчи мослик (обратная совместимость)*. Гибрид схемани мавжуд схеманинг калит тарқатиш маркази процедура ва дастур таъминотида минимал ўзгартиришлар кўзда тутган кенгайтмаси кўринишида осонгина тадбиқ этиш мумкин.

Ошкора калит билан шифрлаш босқичини қўшиш асосий калит тақсимоти воситасини муҳофазасини ва самарадорлигини таъминлайди. Бу эса битта калит тақсимоти марказининг кўплаб бир-биридан етарлича узоқ масофада жойлашган иштирокчиларга хизмат кўрсатгандаги афзаллигидир.

1.3. Носимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари

1.3.1. Диффи-Хеллман алгоритми

У. Диффи ва М. Хеллман тарихда биринчи очиқ калитли алгоритм бўлиб, у 1976 йилда ишлаб чиқилган. Унинг хавфсизлиги (криптобардошлилги) чекли майдонда дискрет логарифмлаш муаммоларини ечиш қийинлигига асосланган.

Диффи-Хеллман алгоритмидан **А** иштирокчи ва **В** иштирокчи ўртасида калитларни тақсимлаш алгоритми сифатида калитни генерация қилишда ишлатилиши мумкин, аммо маълумотларни шифрлаш ва дешифрлашда ишлатиб бўлмайди.

Диффи-Хеллман алгоритмининг математикаси содда. Аввал **А** иштирокчи ва **В** иштирокчи биргаликда катта туб n ва g сонларни танлашади. Бу икки туб сон махфий сақланиши шарт эмас, **А** ва **В** иштирокчилар очиқ махфий булмаган канал орқали келишиб олиши мумкин. Бу сонлар ҳатто фойдаланувчилар гуруҳида биргаликда ҳам (барча фойдаланувчилар учун умумий) ишлатилиши мумкин.

Кейин қуйидаги протокол амалга оширилади (7-расм):

1. **А** иштирокчи ихтиёрий катта туб сон x ни танлайди ва **В** иштирокчига жўнатади:

$X = g^x \bmod n.$

2. **В** иштирокчи ҳам ихтиёрий катта туб сон y ни танлайди ва **А** иштирокчига жўнатади:

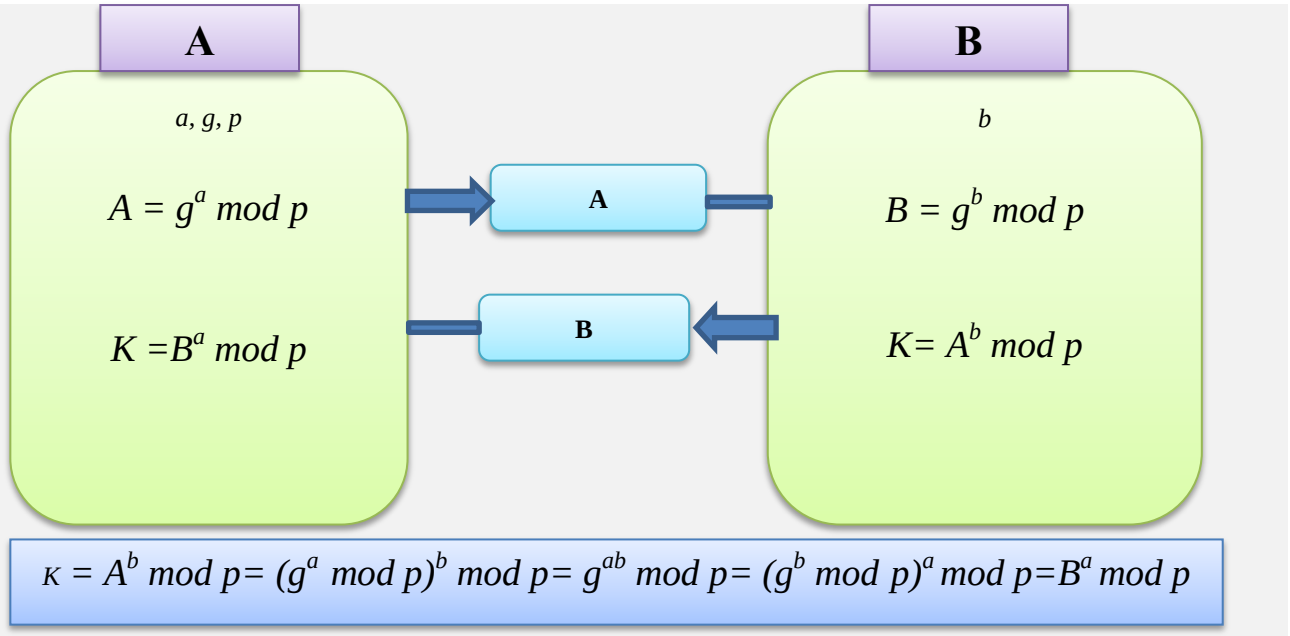
$Y = g^y \bmod n/$

3. **А** иштирокчи қуйидагини ҳисоблайди:

$k = Y^x \bmod n = g^{xy} \bmod n.$

4. **В** иштирокчи эса қуйидагини ҳисоблайди:

$k' = X^y \bmod n = g^{xy} \bmod n.$



7-расм. Диффи-Хеллман алгоритми

Бу ерда *k* ва *k'* тенг *(k=k')*. Ҳеч қандай ўртада кузатиб турган учинчи киши бу қийматни ҳисоблаб топа олмайди, чунки унга фақат *n, g, X* ва *Y* лар маълум. Қачонки улар дискрет логарифм муммосини ечиб *x* ва *y* ларни топа олмас эканлар, улар бу муаммони ҳам ҳал эта олмайдилар. Чунки бу ерда *k* – махфий калитни **A** иштирокчи ва **B** иштирокчи бир-биридан мустақил равишда ҳисоблайди. *n* ва *g* ни танлаш ҳам тизим хавфсизлигига катта таъсир кўрсатади. *(n-1)/2* сони ҳам туб сон бўлиши керак. Ва энг муҳими *n* жуда катта туб сон бўлиши керак, чунки тизим хавфсизлиги шу ўлчамдаги сонларни туб кўпайтувчиларга ажратиш муаммосига асосланган. *g* учун ҳар қандай сон олиниши мумкин, чунки *g* барча ҳолларда модуль *(mod n)* бўйича ҳисобланади. (Аслини олганда *g* ҳам кичкина бўлмаслиги керак, унинг ҳам етарли даражада катта сон бўлиши хавфсизликни таъминлаб беришда муҳим аҳамиятга эга).

1.3.2. Уч ва ундан ортиқ фойдаланувчилар иштирокидаги Диффи-Хеллман алгоритми

Диффи-Хеллман калитларни тақсимлаш протоколини осонгина уч ва ундан ортиқ иштирокчилар учун кенгайтириш мумкин. Масалан,

A иштирокчи, **B** иштирокчи ва **C** иштирокчи биргаликда махфий калитларни генерация қиляпти.

1. **A** иштирокчи ихтиёрий катта сон x ни танлайди ва қуйидагини ҳисоблайди:

$X = g^x \bmod n.$

2. **B** иштирокчи ихтиёрий катта сон y ни танлайди ва қуйидагини ҳисоблайди:

$Y = g^y \bmod n,$

ва уни **C** иштирокчига жўнатади.

3. **C** иштирокчи ихтиёрий катта сон z ни танлайди ва қуйидагини ҳисоблайди:

$Z = g^z \bmod n,$

ва уни **A** иштирокчига жўнатади.

4. **A** иштирокчи **B** иштирокчига жўнатади:

$Z' = Z^x \bmod n.$

5. **B** иштирокчи **C** иштирокчига жўнатади:

$X' = X^y \bmod n.$

6. **C** иштирокчи **A** иштирокчига жўнатади:

$Y' = Y^z \bmod n.$

7. **A** иштирокчи қуйидагини ҳисоблайди:

$k = Y'^x \bmod n.$

8. **B** иштирокчи қуйидагини ҳисоблайди:

$k = Z'^y \bmod n.$

9. **C** иштирокчи қуйидагини ҳисоблайди:

$k = X'^z \bmod n.$

Махфий калит $k = X'^z \bmod n$ га тенг бўлади ва ҳеч қандай ўртадаги кишилар бу қийматни ҳисоблай олмайдилар. Протоколни тўрт ва ундан ортиқ қатнашувчилар учун осон кенгайтирш мумкин, фақат фойдаланувчилар ва ҳисоблаш босқичлари ошади.

1.3.3. Hughes алгоритми

Hughes алгоритми Диффи-Хеллман алгоритмининг ўзгартирилган варианти ҳисобланади. Hughes алгоритми қуйидаги тартибда амалга оширилади (8-расм):

1. **A** иштирокчи катта туб сон x ни генерация қилади ва қуйидагини ҳисоблайди:

$k = g^x \bmod n.$

2. **B** иштирокчи катта туб сон y ни генерация қилади ва қуйидагини ҳисоблаб уни **A** иштирокчига жўнатади:

$Y = g^y \bmod n.$

3. **A** иштирокчи **B** иштирокчига қуйидагини жўнатади:

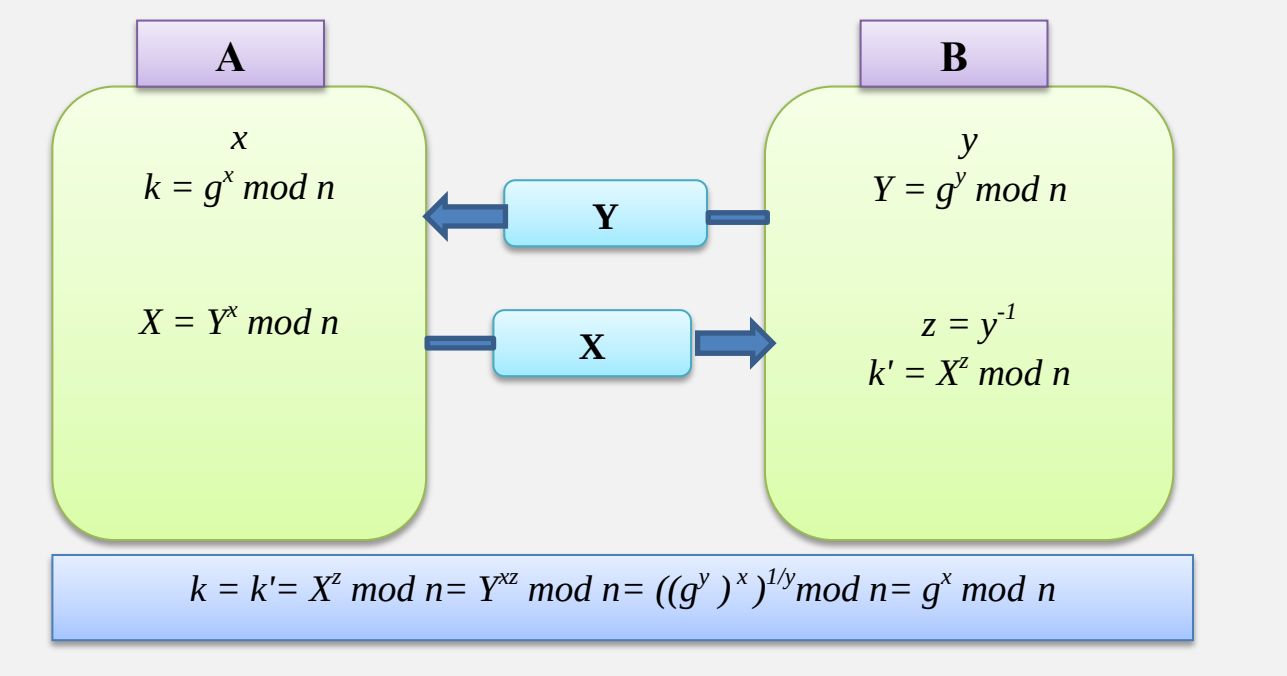
$X = Y^x \bmod n.$

4. **B** иштирокчи қуйидагини ҳисоблайди:

$z = y^{-1}$,

$k' = X^z \bmod n.$

Агар ҳаммаси тўғри бажарилган бўлса, $k = k'$ бўлади.



8-расм. Hughes алгоритми

Hughes протоколининг Диффи-Хеллман протоколидан афзаллиги, k махфий сеанс калитини боғланиш бўлмасдан аввал ҳисоблаб қўйиш мумкин ва бу калит орқали **A** иштирокчи маълумотларни шифрлаб қўйиши мумкин бўлади, яъни **B** иштирокчи билан боғланмасдан туриб амалга ошириши мумкин.

У шифрланган маълумотни бир вақтнинг ўзида бир неча кишига жўнатиши мумкин, калитни эса кейинроқ ҳар бирига алоҳида-алоҳида жўнатиши мумкин.

1.3.4. MTI протоколи

MTI протоколининг номи унинг муаллифлари ҳисобланган *Т. Мацумото И. Такашима ва Х. Имаи*лар шарафига қўйилган. Бу протокол ҳам Диффи-Хеллман протоколига ўхшаш бўлиб, унинг криптобардошлилиги чекли майдонда дискрет логарифмлашга асосланган [14, 20]. Бироқ ундан фарқли томони шундаки, MTI протоколида криптобардошлилигини ошириш мақсадида қўшимча a ва b ўзгарувчилардан фойдаланилади. Ушбу протоколнинг амаллар кетма-кетлиги қуйидагича бажарилади (9-расм). Энг аввало **A** ва **B** иштирокчилар катта туб сон p ва унинг примитив илдизи α нинг қиймати ҳақида келишиб оладилар.

A иштирокчи ўз махфий калити a, $1 \le a \le p-2$ ни генерация қилади ва бу калит ёрдамида

$$z_A = \alpha^a \bmod p$$

ифодани ҳисоблайди. **A** иштирокчи ҳосил бўлган қийматни **B** иштирокчига узатади:

$$\mathbf{A} \to \mathbf{B}: \; z_A = \alpha^a \bmod p,$$

B иштирокчи бу маълумотни қабул қилади. У ўзининг ёпиқ калити b, $1 \le b \le p-2$ ни генерация қилади. Бу ёпиқ калит ёрдамида

$$z_B = \alpha^b \bmod p$$

ифодани ҳисоблайди ва натижани **A** иштирокчига узатади:

$$\mathbf{B} \to \mathbf{A}: \; z_B = \alpha^b \bmod p.$$

A иштирокчи z_B ни қабул қилади. **A** ва **B** иштирокчилар умумий махфий калитни генерация қилиш учун мос ҳолда ўзларининг x, $1 \le x \le p-2$ ва y, $1 \le y \le p-2$ тасодифий сонларини генерация қилишлари зарур. **A** иштирокчи ўзининг тасодифий x сонини генерация қилиб,

$$\alpha^x \bmod p$$

ифодани ҳисоблайди ва уни **B** иштирокчига узатади:

$$\mathbf{A} \to \mathbf{B}: \; \alpha^x \bmod p.$$

B иштирокчи бу маълумотни қабул қилади. У ўзининг тасодифий y сонини генерация қилиб, $\alpha^y \bmod p$ ифодани ҳисоблайди. Ҳосил бўлган натижани **A** иштирокчига узатади. Шу вақтдан бошлаб, **B** иштирокчи α^x ва z_A маълумотларга эга. Энди у ўзининг тасодифий сони ва ёпиқ калитидан фойдаланиб қуйидаги ифодани ҳисоблайди:

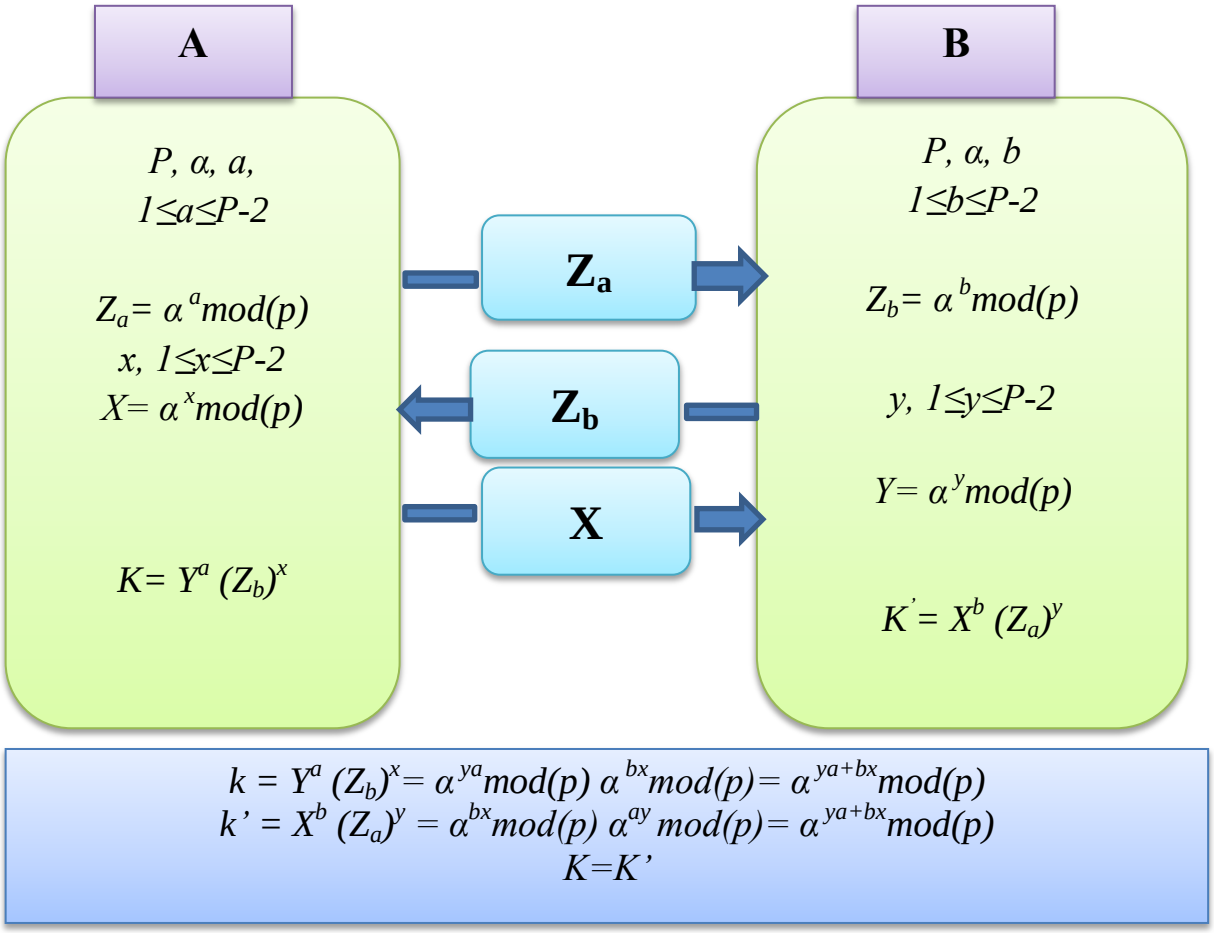
$$k = (\alpha^x)^b \cdot z_A^y ,$$

B → A: $\alpha^y \bmod p$.

A иштирокчи бу маълумотни қабул қилади. Энди **A** иштирокчи α^y ва z_B маълумотларга эга. У ўзининг тасодифий сони ва ёпиқ калитидан фойдаланиб ушбу ифодани ҳисоблайди: $k = (\alpha^y)^a \cdot z_B^x$.

Натижавий калитнинг умумий кўриниши эса қуйидагича:

$$k = (\alpha^y)^a \cdot z_B^x = (\alpha^x)^b \cdot z_A^y = \alpha^{xb+ya} \bmod p .$$



9-расм. MTI протоколи

MTI протоколи шу тартибда амалга оширилади. Унда криптотаҳлилчининг ихтиёрий алмаштириши томонлардаги калитнинг

қиймати турлича бўлишига олиб келади. Бу эса узатилаётган маълумотни ўқиш имкониятини бутунлай йўқотади.9-расм. MTI протоколи

Қуйида MTI пртоколи учун ҳам мисол келтирилади.

$p = 9531$

$\alpha = 1647$

$A:\ a = 126$

$A:\ Z_a = \alpha^a \bmod p = 1647^{126} \bmod 9531 = 3375$

$A \to B:\ Z_a = 3375$

$B:\ b = 98$

$B:\ Z_B = \alpha^b \bmod p = 1647^{98} \bmod 9531 = 8775$

$B \to A:\ Z_B = 8775$

$A:\ x = 8643$

$A:\ X = \alpha^x \bmod p = 1647^{8643} \bmod 9531 = 972$

$A \to B:\ X = 972$

$B:\ k_1 = (\alpha^x)^b Z_A^y \bmod p = X^b Z_A^y \bmod p = 972^{98} \cdot 3375^{6983} \bmod 9531 = 3564$

$B:\ y = 6983$

$B:\ Y = \alpha^y \bmod p = 1647^{6983} \bmod 9531 = 4131$

$B \to A:\ Y = 4131$

жавоб: $k_1 = k_2 = k = 3564$.

1.3.5. DASS протоколи

DASS протоколи калит тақсимоти ва аутентификациясининг ИМ иштирокидаги симметрик ва носимметрик алгоритмларга асосланган протоколдир [10-12]. Бунда **A** ва **B** иштирокчилар ҳамда ИМ S ўзларининг очиқ ва ёпиқ калитлари жуфтига эгалар, яъни k_a, k_b, k_s ўзаро мос ҳолатда. Бу калитлар билан мос равишда хабарларни имзолаш s_a, s_b, s_S.

DASS протоколи схемасини қуйидаги келтирилади (10-расм):

$A \to S: B,$

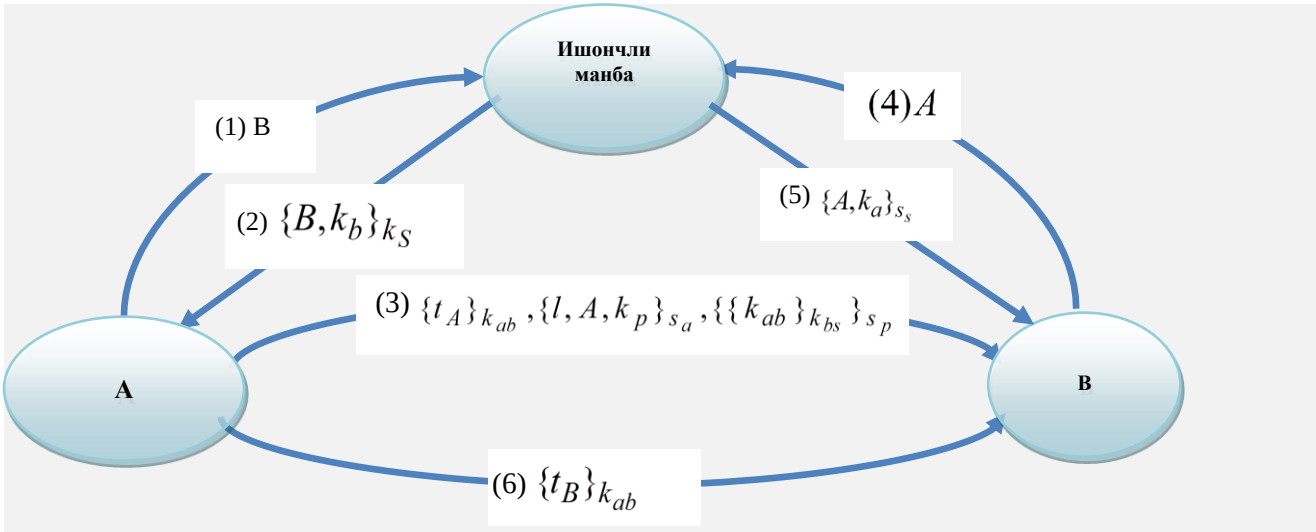
$S \to A: \{B, k_b\}_{k_s}$,

$A \to B: \{t_A\}_{k_{ab}}, \{l, A, k_p\}_{s_a}, \{\{k_{ab}\}_{k_{bs}}\}_{s_p}$,

$B \to S: A,$

$S \to B : \{A, k_a\}_{s_s}$,

$B \to A : \{t_B\}_{k_{ab}}$.



10-расм. DASS протоколи

DASS протоколининг тўлиқ баёни қуйида келтирилади:

– **A** иштирокчи ИМга **B** иштирокчининг очиқ калитини олиш учун сўровнома юборади.

– ИМ **B** иштирокчининг калити k_b ни ўзининг калити билан имзолаб узатади.

– **A** иштирокчи маълумотларни ИМнинг аввалдан маълум бўлган очиқ калити билан текширади, сўнгра сеанс калити k_{ab} ни ва тасодифий сеанс катити k_p ни генерация қилади, ВБ t_a ни ва калитнинг яроқлилик муддатини қўшиб, бир қисмини шифрлаб, бир қисмини имзолаб **B** иштирокчига юборади.

– **B** иштирокчи ИМга **A** иштирокчининг идентификаторини олиш учун сўровнома юборади.

– ИМ **B** иштирокчининг калитини ўзининг калити билан имзолаб юборади.

– **A** иштирокчининг ва ИМнинг хабарларидаги маълумотлардан фойдаланиб, **B** иштирокчи **A** иштирокчининг имзосини текширади, тасодифий сеанс калити k_p ни, сеанс калити k_{ab} ни чиқариб олади ва t_A

нинг шифрини очиб такрорланганидан эмас, балки шу вақтдаги хабардан фойдаланилаётганига ишонч ҳосил қилади.

– Заруратга кўра протокол томонларни ўзаро идентификациясини таъминлаш мақсадида давом эттирилиши мумкин.

1.3.6. Деннинг – Сакко протоколи

Деннинг–Сакко *(Denning-Sacco)* протоколи ошкора калитли аутентификациялаш ва калит тақсимлаш протоколи бўлиб, DASS протоколидаги каби ИМ барча очиқ калитларнинг маълумотлар базасини тутиб туради [3-6, 17].

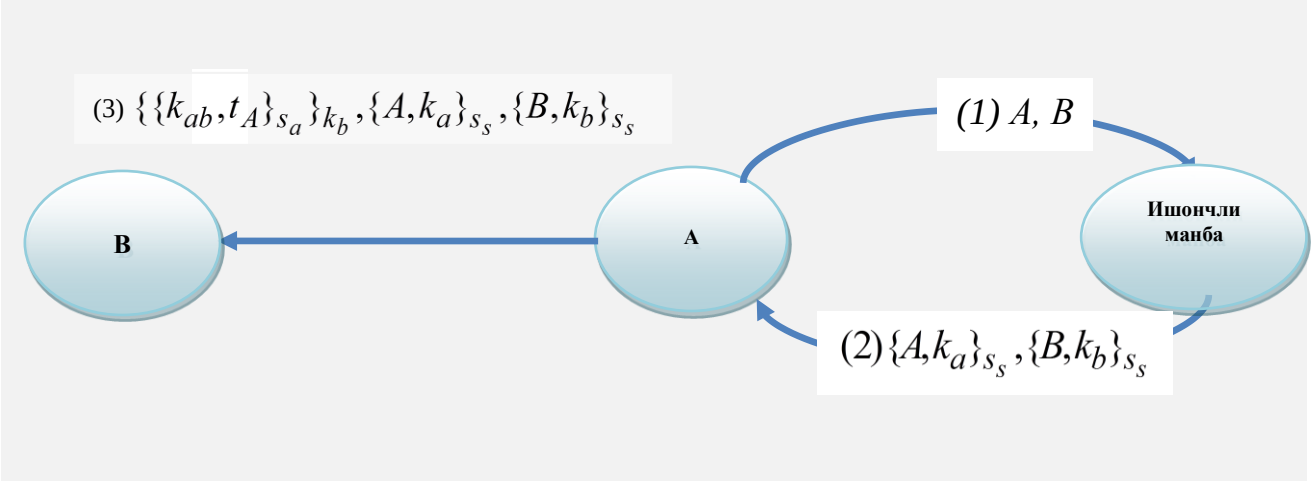
Деннинг–Сакко протоколининг заифлиги шундан иборатки, томонлардан бири сеанс тугагандан сўнг ўзини бошқа томондан деб кўрсатиш имкониятига эга.

Деннинг– Сакко протоколининг схемаси (11-расм) :

$A \to S : A, B,$

$S \to A : \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$

$A \to B : \{\{k_{ab}, t_A\}_{s_a}\}_{k_b}, \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$



11-расм. Деннинг – Сакко протоколи

– **A** иштирокчи ИМга ўзининг ва **B** иштирокчининг идентификаторини юборади.

– ИМ **A** иштирокчига ўзининг махфий калити билан имзолаган **A** ва **B** иштирокчиларнинг очиқ калитларини ва идентификаторларини узатади.

– **A** иштирокчи сеанс калити ва вақт белгисини ўзининг калити билан имзолаб, сўнгра уни **B** иштирокчининг очиқ калити билан шифрлаб ва ИМнинг хабари билан тўлдириб **B** иштирокчига юборади.

– **B** иштирокчи хабарни шифрини очиб, ИМнинг очиқ калитидан фойдаланиб калитлардаги имзони текширади, **A** иштирокчининг очиқ калитидан фойдаланиб сеанс калитидаги имзони текширади, бунда сеанс калити k_{ab} дан **A** иштирокчи билан хавфсиз маълумот алмашинувида фойдаланиши мумкин бўлади.

A иштирокчидан келган хабарда $\{\{k_{ab},t_A\}_{s_a}\}_{k_b}$ олувчининг идентификатори қатнашмаслиги, **B** иштирокчига **A** иштирокчидан олган маълумотларни бошқа иштирокчи билан бўладиган янги сеансда ўзини **A** иштирокчи деб кўрсатиши имконини беради. Бу муаммони хабарга **A** ва **B** иштирокчиларнинг идентификаторини қўшиб, яъни бу хабарни ишлатилишини фақат шу сеанс билан чегаралаб осон ҳал қилиш мумкин.

1.3.7. Ву – Лама протоколи

Ву – Лама *(Woo-Lam)* протоколи ҳам Деннинг – Сакко протоколи каби ошкора калитли аутентификациялаш ва калит тақсимлаш протоколи бўлиб [3-6, 17], DASS протоколидаги каби ИМ барча очиқ калитларнинг маълумотлар базасини тутиб туради.

Ву – Лама протоколи схемаси 12-расмда келтирилган:

$A \to S : A, B,$

$S \to A : \{k_b\}_{s_s}$,

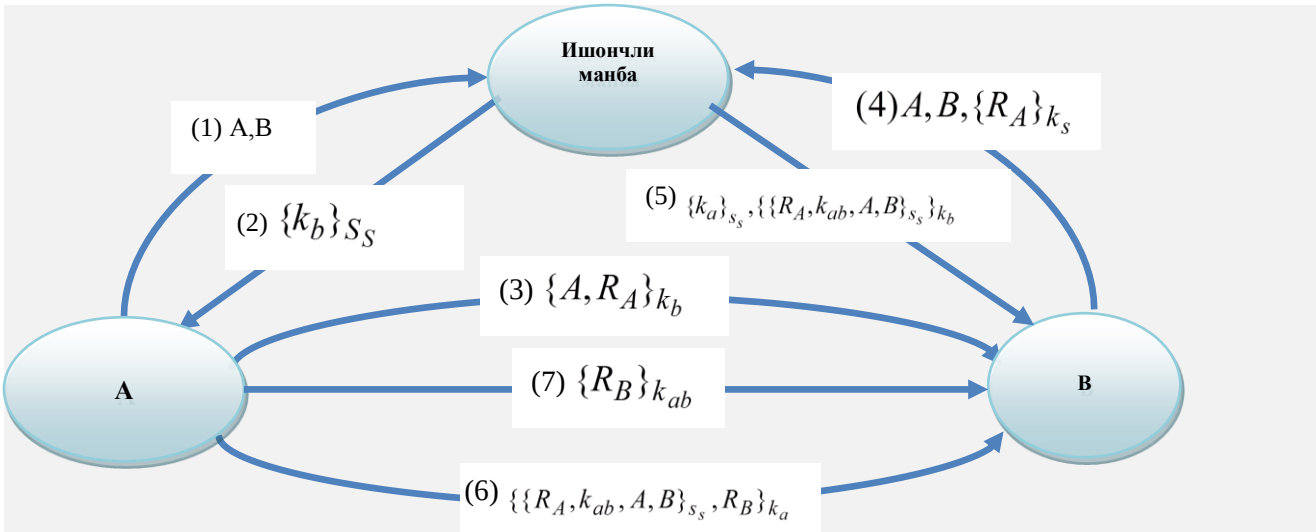
$A \to B : \{A, R_A\}_{k_b}$,

$B \to S : A, B, \{R_A\}_{k_s}$,

$S \to B : \{k_a\}_{s_s}, \{\{R_A, k_{ab}, A, B\}_{s_s}\}_{k_b}$,

$B \to A : \{\{R_A, k_{ab}, A, B\}_{s_s}, R_B\}_{k_a}$,

$A \to B : \{R_B\}_{k_{ab}}$.



12-расм. Ву – Лама протоколи

Энди Ву – Лама протоколининг тўлиқ баёнини келтирамиз:

– **А** иштирокчи ИМга ўзининг ва **В** иштирокчининг идентификаторини юборади.

– ИМ **А** иштирокчига ўзининг махфий калити билан имзолаган В иштирокчининг очиқ калитларини узатади.

– **А** иштирокчи имзони текширади, сўнгра **В** иштирокчига ўзининг идентификатори ва тасодифий танланган сонни **В** иштирокчининг очиқ калити билан шифрлаб юборади.

– **В** иштирокчи эса ИМга ўзининг ва **А** иштирокчининг идентификаторини ва тасодифий танлаган сонни ИМнинг очиқ калити билан шифрлаб узатади.

– ИМ **В** иштирокчига иккита хабар юборади. Биринчисида **А** иштирокчининг ИМнинг калити ёрдамида имзоланган очиқ калити бўлса, иккинчисида ИМ калити билан имзоланган ва **В** иштирокчининг очиқ калити билан шифрланган **А** иштирокчининг тасодифий танлаган сони, тасодифий танланган сеанс калити ва **А** ва **В** иштирокчиларнинг идентификатори бўлади.

– **В** иштирокчи ИМ очиқ калити ёрдамида хабарнинг ҳақиқийлигини текширади, сўнгра **А** иштирокчига ИМ хабарининг иккинчи қисмини, унинг имзоси билан, ўзининг тасодифий танлаган сони билан тўлдириб **А** иштирокчининг очиқ калити билан шифрлаб юборади.

– **A** иштирокчи ИМ имзосини ва ўзининг тасодифий танлаган сонининг тенглигини текширади, сўнгра **B** иштирокчига **B** тасодифий танлаган сонни унинг сеанс калити билан шифрлаб қайта юборади.

– **B** иштирокчи соннинг шифрини очиб унинг ўзгармаганлигига ишонч ҳосил қилади.

Носимметрик алгоритмларга асосланган калитларни тақсимлаш протоколларига юқорида келтирилган протоколлардан ташқари COMSET (Communications Setup, алоқа ўрнатиш), EKE (Encrypted Key Exchange, шифрланган калитлар билан алмашиш) протоколлари ва SKEY (маълумотнинг ҳақиқийлигини текширувчи) дастури мавжуд бўлиб улардан маълумотнинг хавфсизлигини таъминлаш учун фойдаланиш мумкин.

1.4. Симметрик криптотизимларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари

1.4.1. Шамир протоколи

Симметрик криптотизимлардан муваффақиятли фойдаланиш учун махфий калит тўғрисида келишиб олиш, яъни турли иштирокчилар ўртасида калитлар тақсимланган бўлиши керак.

Қуйида **Шамир протоколи** деб аталувчи (калитсиз) умумий махфий маълумотдан фойдаланмаган ҳолда калитни узатиш протоколини кўриб чиқилади. Бу протокол қадамларига мувофиқ калитнинг махфийлик масаласи таъминланади.

Шундай шифрлаш ва дешифрлаш ўзгартиришлари мавжудки [2,14] барча x маълумотлар, k_1 ва k_2 калитлар учун қуйидаги шарт бажарилади:

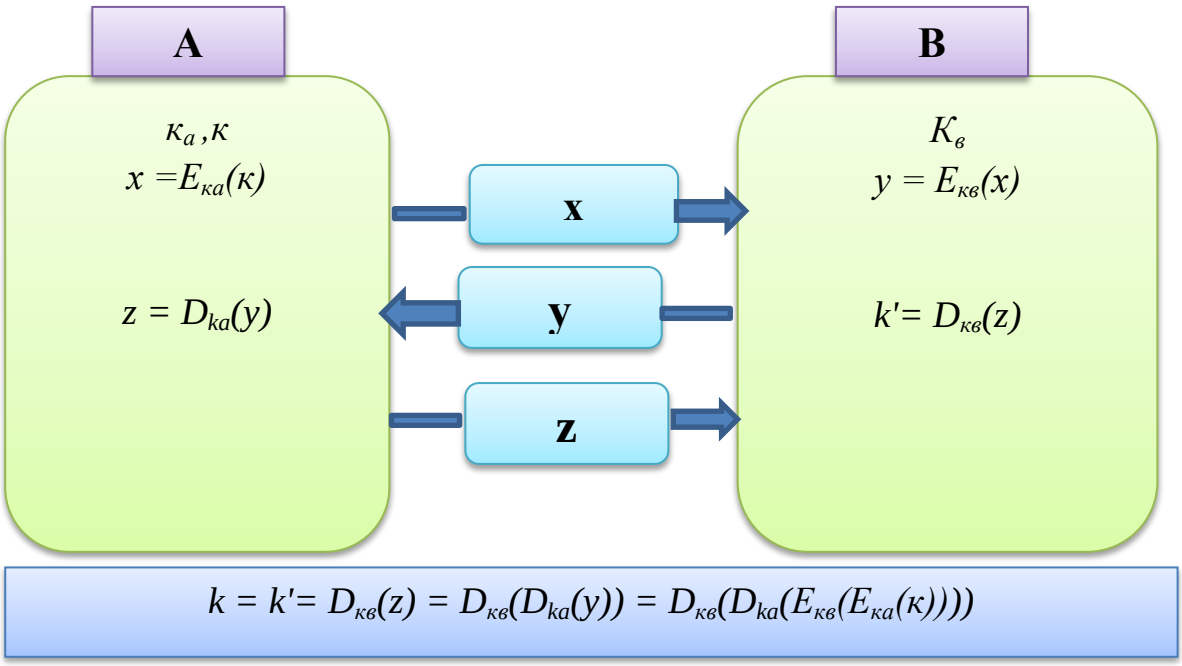
$$E_{k_1}(E_{k_2}(x)) = E_{k_2}(E_{k_1}(x)).$$

У ҳолда **A** ва **B** иштирокчилар k сеанс калитини узатувчи қуйидаги 3-босқичли протоколдан фойдаланишлари мумкин:

1. $\mathbf{A} \rightarrow \mathbf{B}$: $E_{k_A}(k)$,

2. **B** $\rightarrow$ **A :** $E_{k_B}(E_{k_A}(k))$,

3. **A** $\rightarrow$ **B:** $D_{k_A}(E_{k_B}(E_{k_A}(k)))$.



13-расм. Шамир протоколи

Хусусан, Шамир протоколида модуль бўйича даражага кўтариш амалидан фойдаланиш таклиф этилган, яъни $E_{k_A}(k) = k^{k_A} \bmod p$. Шундай қилиб, бу протоколнинг криптобардошлиги дискрет логарифмлаш масаласининг мураккаблигига асосланган [2, 20]. Шамир протоколининг камчилиги шундаки, бу протоколда аутентификация масаласи ҳал этилмаган.

1.4.2. Нидхем-Шрёдер протоколи

Рожер Нидхем ва Михаэл Шрёдерлар томонидан яратилган бу протоколда арбитр ва симметрик криптотизимдан фойдаланилади (14-расм):

1. **A** иштирокчи ишончли томонга (**W**) ўзининг исмини, **B** иштирокчининг исмини ва ўзининг тасодифий сонини узатади.

A $\rightarrow$ **W :** A, B, R_A .

2. 3-ишончли томон сеанс калитни генерация қилади. Бу сеанс калитни ва **A** иштирокчининг исмини **B** иштирокчи билан умумий бўлган калит орқали шифрлайди. Сўнгра **A** иштирокчи ва ўзи учун умумий бўлган калит

ёрдамида **A** иштирокчининг тасодифий сони, **B** иштирокчининг исми, калит ва шифрматнни шифрлайди. Ниҳоят у шифрланган маълумотни **A** иштирокчига узатади:

W → B : $E_A(R_A, B, k, E_B(k, A))$.

3. **A** иштирокчи маълумотни дешифрлаб, k калитни олади. У R_A ва 1-босқичда узатилган R_A ни солиштиради. Сўнгра **A** иштирокчи ишончли томон шифрлаган маълумотни **B** иштирокчига узатади:

A → B : $E_B(k, A)$.

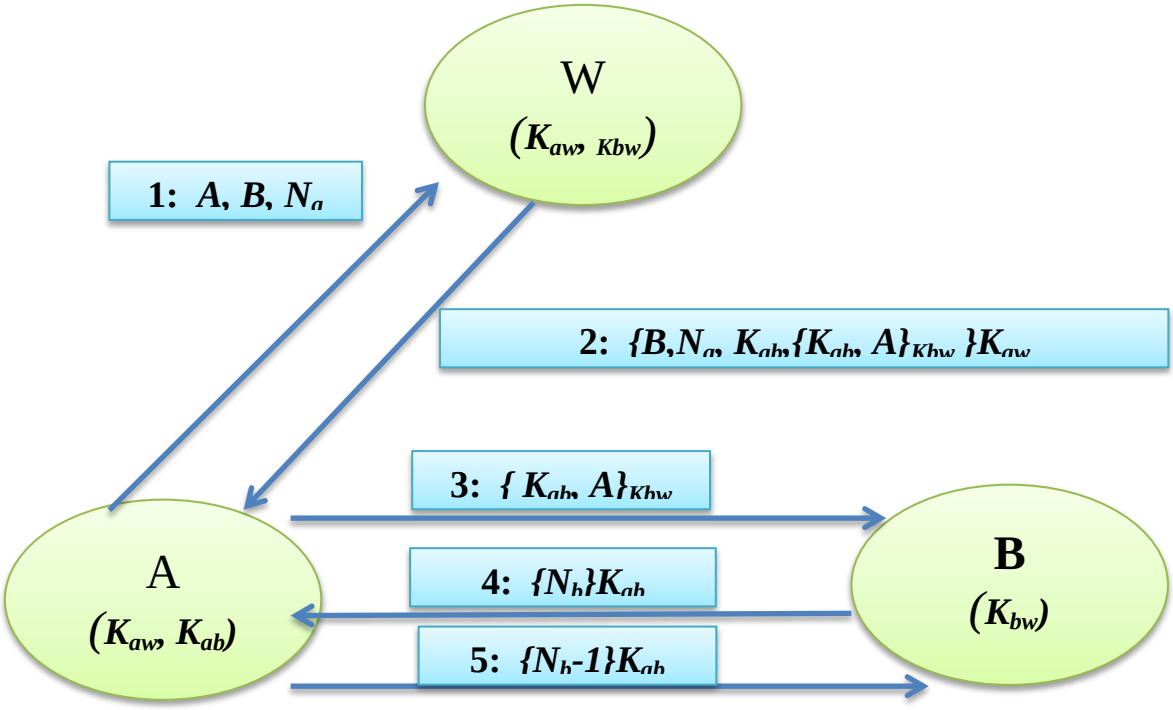
4. **B** иштирокчи бу маълумотни дешифрлайди ва k калитни олади. Сўнгра у тасодифий R_B сонини генерация қилади. Бу тасодифий сонни k калит ёрдамида шифрлайди ва **A** иштирокчига узатади:

B → A : $E_k(R_B)$.

5. **A** иштирокчи k калит ёрдамида маълумотни дешифрлайди. **A** иштирокчи тасодифий $R_B - 1$ сонини генерация қилади. Бу сонни k калит ёрдамида шифрлаб қайта **B** иштирокчига узатади:

A → B : $E_k(R_B - 1)$.

6. **B** иштирокчи маълумотни дешифрлаб, $R_B - 1$ сонини текширади ва ҳақиқатдан **A** иштирокчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.



14-расм. Нидхем-Шрёдер протоколи

Бу протоколда R_A, R_B ва $R_B - 1$ сонларидан такроран фойдаланилади. Агар криптотаҳлилчи аввал фойдаланилган k калитни қўлга киритса, 3-босқичда **A** иштирокчи номидан **B** иштирокчига маълумот узатиши мумкин.

1.4.3. Wide-Mouth Frog протоколи

Wide-Mouth Frog протоколини ишончли сервер учун фойдаланиладиган калитларни алмашувчи симметрик протокол дейиш мумкин. **A** ва **B** иштирокчилар арбитр билан биргаликда умумий калитлардан фойдаланадилар. Wide-Mouth Frog протоколида **A** иштирокчи **B** иштирокчига сеанс калитни қуйидагича узатади (15-расм):

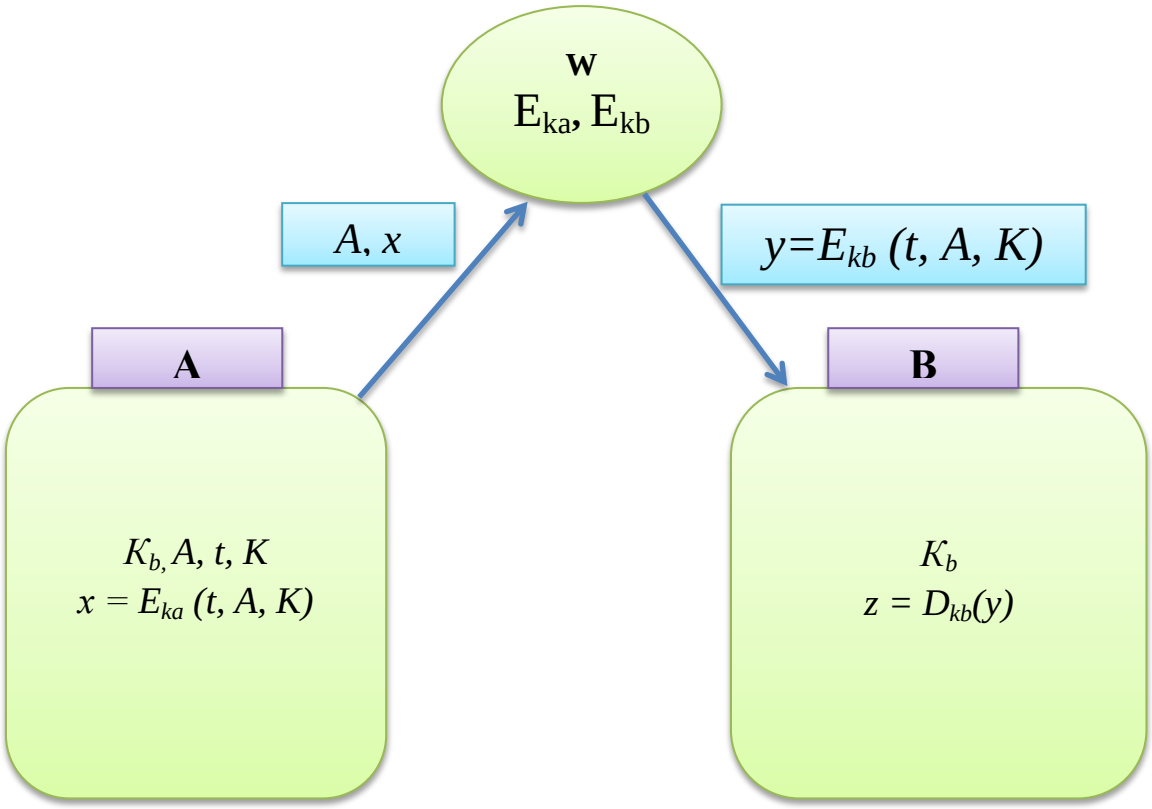
1. **A** иштирокчи вақт белгисини, **B** иштирокчининг исмини ва сеанс калитни бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва шифрматнни арбитр (**W**) га узатади:

$$\mathbf{A} \to \mathbf{W}: \; A, E_A(t, A, k).$$

2. Арбитр **A** иштирокчининг маълумотини дешифрлайди. Сўнгра янги вақт белгисини, **A** иштирокчининг исмини ва сеанс калитни бирлаштириб ўзи ва **B** иштирокчи учун умумий бўлган калит билан шифрлайди. Натижани **B** иштирокчига узатади:

$$\mathbf{W} \to \mathbf{B}: \; E_B(t, A, k).$$

3. **B** иштирокчи бу маълумотни қабул қилиб умумий калит билан дешифрлайди ва вақт белгисини олиб, қабул қилган вақти билан солиштиради. Агар бу вақтлар орасидаги фарқ белгиланган интервалдан ошмаса, k калитни ҳақиқий деб қабул қилади.



15-расм. Wide-Mouth Frog протоколи

1.4.4. Yahalom протоколи

Yahalom протоколига мувофиқ **A** ва **B** иштирокчилар арбитр билан умумий калитдан фойдаланадилар. Протокол қадамлари кетма-кетлиги қуйидагидан иборат:

1. **A** иштирокчи ўзи исми ва тасодифий сонини бирлаштириб, **B** иштирокчига узатади:

$$\mathbf{A} \rightarrow \mathbf{B}: \ A, R_A \ .$$

2. **B** иштирокчи **A** иштирокчининг исмини, унинг тасодифий сонини ва ўзининг тасодифий сонини бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва натижани бирлаштириб арбитрга узатади:

$$\mathbf{B} \rightarrow \mathbf{W}: \ B, E_B(A, R_A, R_B) \ .$$

3. Арбитр иккита маълумотни ҳосил қилади. Биринчи маълумот **B** иштирокчининг исми, сеанс калит, **A** ва **B** иштирокчиларнинг тасодифий сонларидан ташкил топган. Бу маълумотни ўзининг ва **A** иштирокчининг

умумий калити билан шифрлайди. Иккинчи маълумот **A** иштирокчининг исми ва сеанс калитидан ташкил топган. Арбитр бу маълумотни ўзи ва **B** иштирокчи учун умумий бўлган калит билан шифрлайди. Сўнгра бу маълумотларни **A** иштирокчига узатади:

$$\mathbf{W \to A:}\ E_A(B, k, R_A, R_B), E_B(A, k)\ .$$

4. **A** иштирокчи биринчи маълумотни дешифрлайди ва k калитни олади. У R_A ни 1-босқичда узатилган қиймати билан солиштиради ва тўғри эканлигига ишонч ҳосил қилади. Сўнгра **A** иштирокчи **B** иштирокчига иккита маълумот узатади, биринчи – арбитрнинг маълумоти, иккинчиси – сеанс калит билан шифрланган R_B - тасодифий сон:

$$\mathbf{A \to B:}\ E_B(A, k), E_k(R_B)\ .$$

5. **B** иштирокчи биринчи маълумотни дешифрлаб, k калитни олади. Бу калит ёрдамида иккинчи маълумотни очиб, R_B нинг қиймати 2-босқичда юборилгани билан мос келишига ишонч ҳосил қилади.

Натижада **A** ва **B** иштирокчилар айнан бир-бирлари билан алоқа боғлаганларига ишонч ҳосил қиладилар.

1.4.5. Отвей-Риис протоколи

Бу протоколда ҳам симметрик шифрлаш алгоритмидан фойдаланилади. Протокол қадамлари кетма-кетлиги қуйидагича:

1. **A** иштирокчи тартиб рақами, ўзининг исми, **B** иштирокчининг исми ва тасодифий R_A сонидан ташкил топган маълумотни ҳосил қилади ва уни шифрлайди. Сўнгра у шифрматнни, тартиб рақамини, ўзининг ва **B** иштирокчининг исмини **B** иштирокчига узатади:

$$\mathbf{A \to B:}\ I, A, B, E_A(R_A, I, A, B)\ .$$

2. **B** иштирокчи тасодифий R_B сони, тартиб рақами, **A** иштирокчи ва ўзининг исмидан ташкил топган маълумотни ҳосил қилади. Бу маълумот умумий калит билан шифрланади. Сўнгра **B** иштирокчи бу маълумотни, **A** иштирокчи юборган маълумотни, тартиб рақами, ўзи ва **A** иштирокчининг исмини арбитрга узатади:

$$\mathbf{B \to W:}\ I, A, B, E_A(R_A, I, A, B), E_B(R_B, I, A, B)\ .$$

3. Арбитр тасодифий сеанс калитини хосил қилади. Сўнгра иккита маълумотни ҳосил қилади, биринчиси – **A** иштирокчининг умумий калити билан шифрланган **A** иштирокчининг тасодифий R_A сони, иккинчиси – **B** иштирокчининг умумий калити билан шифрланган **A** иштирокчининг тасодифий R_A сони. Арбитр тартиб рақамини ва иккала маълумотни бирлаштириб **B** иштирокчига узатади:

$$\mathbf{W} \to \mathbf{B}: \; I, E_A(R_A, k), E_B(R_B, k).$$

4. **B** иштирокчи **A** иштирокчининг калити билан шифрлаган тасодифий сон ва k сеанс калитни **A** иштирокчига узатади:

$$\mathbf{B} \to \mathbf{A}: \; I, E_A(R_A, k).$$

5. **A** иштирокчи маълумотни дешифрлаб, ўзининг тасодифий сони ва k сеанс калитига эга бўлади. **A** иштирокчи протокол бажарилиши натижасида улар ўзгармасдан қолганига ишонч ҳосил қилади .

Агар протокол бажарилиши натижасида барча тасодифий сонлар тўғри ва тартиб рақами ўзгармаган бўлса, у ҳолда **A** ва **B** иштирокчилар бир-бирларининг ҳақ эканликларига ишонч ҳосил қиладилар ва ўзаро маълумот алмашиш учун махфий калитни қабул қиладилар.

1.4.6 Ньюман-Стабблбайн протоколи

Ньюман-Стабблбайн протоколи калит тақсимоти ва аутентификациясининг ИМ иштирокидаги симметрик протоколи бўлиб, Яхалом протоколининг такомиллаштирилган русуми ҳисобланади [10]. Ньюман - Стабблбайн протоколининг ўзига хос хусусияти шундан иборатки, унда томонлараро вақтни синхронлаштириш зарурати ва ИМни иштирокисиз такрорий аутентификация қилиш имконияти мавжуд.

Ньюман - Стабблбайн протоколининг схемаси қуйидагича (16-расм):

$A \to B: A, R_A,$

$B \to S: B, R_b, \{A, R_A, t_B\}_{k_{bs}},$

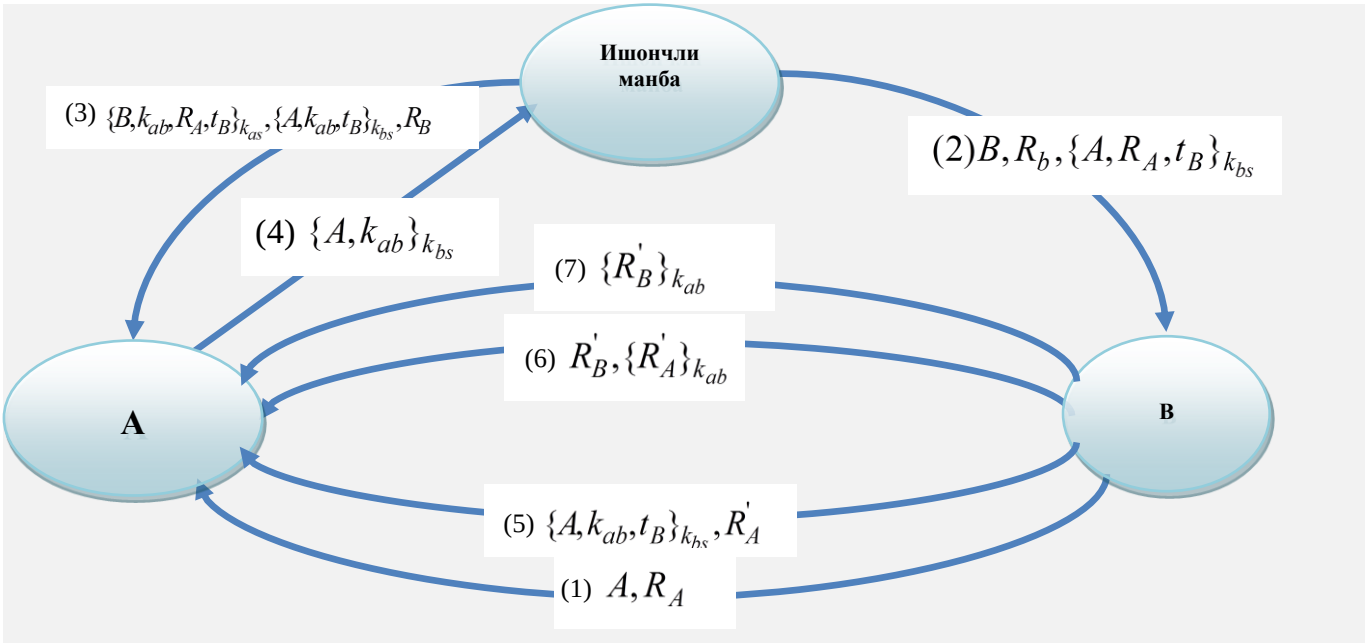
$S \to A: \{B, k_{ab}, R_A, t_B\}_{k_{as}}, \{A, k_{ab}, t_B\}_{k_{bs}}, R_B$

$A \to B: \{A, k_{ab}\}_{k_{bs}}, \{R_B\}_{k_{ab}}$

$A \to B: \{A, k_{ab}, t_B\}_{k_{bs}}, R_A^{'}$

$$B \to A: R_B^{'}, \{R_A^{'}\}_{k_{ab}},$$

$$A \to B: \{R_B^{'}\}_{k_{ab}}.$$



16-расм. Ньюман-Стабблбайн протоколи

A иштирокчи **B** иштирокчига тасодифий танланган сон R_A ни ва ўз идентификаторини юборади.

– **B** иштирокчи хабарни ўзининг ВБ t_B билан тўлдиради, сўнгра k_{bs} калит билан шифрлаб, ўз идентификаторини ва тасодифий танлаган R_B сонни қўшиб ИМга узатади.

– ИМ **B** иштирокчи идентификаторини, **A** иштирокчининг тасодифий танланган сон R_A ни, сеанс калити k_{ab} ни ва t_B ни k_{as} калит билан, А иштирокчидан идентификаторини, сеанс калити k_{ab} ни ва t_B ни k_{bs} калит билан шифрлаб, сўнгра тасодифий танлаган R_B сонни қўшиб **A** иштирокчига юборади.

– **A** иштирокчи R_A ни 1-хабарда ўзи юборгани билан таққослаб, бир хиллигига ишонч ҳосил қилиб, сўнгра ўз идантификаторини ва сеанс калити k_{ab} ни k_{bs} калит билан шифрлаб, унга R_B сонини сеанс калити k_{ab} билан шифрланганини қўшиб **B** иштирокчига узатади.

– **B** иштирокчи ўз навбатида t_B ва R_B қийматларни текшириб, ўзгармаганлигига ишонч ҳосил қилади.

Юқорида айтиб ўтганимиздек, бу протоколда ИМнинг иштирокисиз, янги тасодифий танланган сонлардан фойдаланиб такрорий аутентификация қилиш имконияти мавжуд, яъни

– **A** иштирокчи ўз идентификаторини, сеанс калити k_{ab} ни ва t_B ни k_{bs} калит билан шифрлаб уни янги тасодифий танланган сон $R_A^{'}$ билан тўлдириб **B** иштирокчига юборади.

– **B** иштирокчи янги тасодифий танланган сон $R_A^{'}$ ни сеанс калити k_{ab} билан шифрлаб, уни ўзи тасодифий танлаган янги $R_B^{'}$ билан тўлдириб **A** иштирокчига қайтаради.

– **A** иштирокчи эса ўз навбатида **B** тасодифий танлаган янги $R_B^{'}$ ни сеанс калити k_{ab} билан шифрлаб **B** иштирокчига юборади.

Бунда янги тасодифий танланган $R_A^{'}$ ва $R_B^{'}$ сонлардан фойдаланиш қайта юборишга бўладиган ҳужумдан ҳимоя қилади.

1.5. Калитларни тақсимлаш алгоритмларининг қиёсий таҳлили ва таснифи

Калитларни тақсимлаш бўйича мавжуд хорижий алгоритмларнинг таҳлили шуни кўрсатдики, уларнинг бардошлилигини таъминлашга асос бўлган мураккаб муаммолар қуйидагилардан иборат:

- дискрет логарифм муаммосининг мураккаблигига асосланган;
- Диффи-Хеллман муаммосининг мураккаблигига асосланган;
- эллиптик эгри чизиқ (ЭЭЧ)да дискрет логарифм муаммосининг мураккаблигига асосланган;
- бошқа муаммоларга асосланган алгоритм ва протоколлардир.

Калитларни тақсимлаш бўйича мавжуд алгоритмлар ва протоколларнинг кўпчилиги дискрет логарифмлаш ва ЭЭЧда дискрет логарифмлаш муаммоларининг мураккаблигига асосланган дир.

Охириги йилларда калитларни тақсимлаш алгоритмлари ЭЭЧларга асосланиб ишлаб чиқилмоқда. Шу боис, ЭЭЧда дискрет логарифмлаш муаммосиини ҳал этиш кўпчилик криптотаҳлилчиларнинг эътиборини ўзига тортмоқда.

Калитларни тақсимлаш протоколларига ҳужумлар турлича таъсир қилади. Қуйидаги 1-жадвалда носимметрик алгоритмларга асосланган калитларни тақсимлаш протоколларига қилинадиган ҳужум турлари кўрсатилган.

1-жадвал

Ҳужумларнинг носимметрик калитларни тақсимлаш протоколларига таъсири

№	Протокол номи	Ҳужум турлари
1	**Диффи- Хеллман протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас. Криптотаҳлилчи бу маълумотларни маълум вақтдан кейин **B** иштирокчига қайта жўнатиши мумкин
2	**Уч ва ундан ортиқ фойдаланувчилар иштирокидаги Диффи-Хеллман протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас.
3	**Hughes протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас
4	**MTI протоколи**	Криптотаҳлилчининг ихтиёрий алмаштириши томонлардаги калитнинг қиймати турлича бўлишига олиб келади.
5	**DASS протоколи**	**B** иштирокчи ЭРИни текшириш имконига эга бўлмайди Томонлар ўртасида ўзаро идентификация таъминланмайди
6	**Деннинг – Сакко протоколи**	Протокол якунлангандан сўнг **B** иштирокчи бошқа **C** иштирокчи билан алоқа ўрнатиши учун **A** иштирокчининг номидан иш кўриши мумкин
7	**Ву – Лама протоколи**	**A** иштирокчи арбитрни идентификация қилмайди Иштирокчилар бир-бирини идентификация қилмайдилар

Қуйидаги 2-жадвалда симметрик алгоритмларга асосланган калитларни тақсимлаш протоколларига қилинадиган ҳужум турлари кўрсатилган.

2-жадвал

Ҳужумларнинг симметрик калитларни тақсимлаш протоколларига таъсири

№	Протокол номи	Ҳужум турлари
1	**Шамир протоколи**	Криптотаҳлилчи криптотаҳлил усули орқали калитни аниқлаши мумкин
2	**Нидхейм-Шредер протоколи**	**B** иштирокчи калитни ким томонидан юборилганини билмайди Криптотаҳлилчи бу калитни маълум вақтдан сўнг қайта узатиши мумкин Арбитр маълумотни кимдан келганини ва кимга юбориш кераклиги ҳақида ҳеч нарса билмайди **A** иштирокчи маълумотни арбитрдан келганига тўла ишонч ҳосил қилмайди
3	**Wide-Mouth Frog протоколи**	Криптотаҳлилчи маълумотни **B** иштирокчига такроран узатиши мумкин Иштирокчилар маълумотни кимдан келганини билмайди
4	**Yahalom протоколи**	Иштирокчилар ўртасида ўзаро идентификация таъминланмайди
5	**Отвей-Риис протоколи**	
6	**Ньюман-Стабблбайн протоколи**	“Яширин такрорий узатиш” ҳужуми бўлиши мумкин

Шундай қилиб, калитларни тақсимлаш протоколларидан фойдаланилаётганда протоколларга қилинаётган ҳужумларни албатта инобатга олиш талаб этилади.

Криптографик калитларни тақсимлаш алгоритми ва протоколларини қуйидаги белгилар асосида таснифлаш мумкин:

1. Калит тури.

2. Калитни тақсимлаш вазияти.

3. Калитларни тақсимлаш усули.

4. Калитларни тақсимлаш схемаси.

5. Калитларни тақсимлаш протоколи бардошлилигини таъминловчи муаммо тури.

Қуйидаги 17-расмда криптографик калитларни тақсимлаш протоколларининг таснифи келтирилган.

1-боб бўйича хулосалар

1. Криптотизим қанчалик криптобардошли ва ишончли бўлмасин, ундан амалда фойдаланиш жараёнлари калитларни бошқариш жараёнлари масалалари билан боғлиқлиги асосланди.

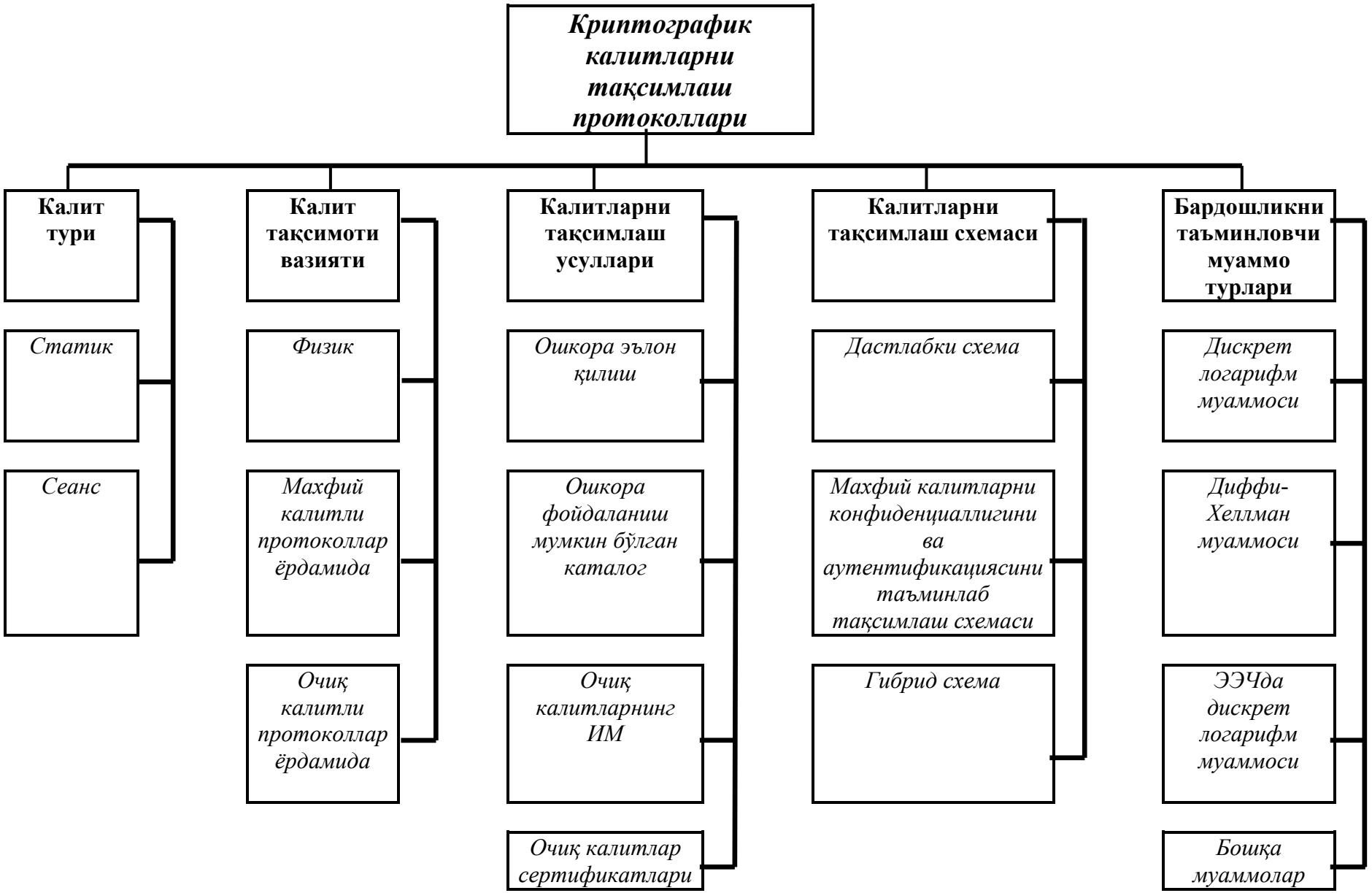
2. Криптографик калитларни тақсимлашнинг замонавий усуллари ва схемалари тадқиқ этилди.

3. Носимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколларидан ҳужжатли маълумотларнинг махфийлигини таъминлаш учун фойдаланиш мумкинлиги изоҳланди.

4. Ҳозирги кунда энг кўп қўлланиладиган хорижий симметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари таҳлил этилди.

5. Калитларни тақсимлаш бўйича мавжуд хорижий алгоритмларнинг таҳлили шуни кўрсатдики, уларнинг кўпчилигининг криптографик бардошлилиги дискрет логарифмлаш ва ЭЭЧда дискрет логарифмлаш муаммоларининг мураккаблигига асослангандир.

6. Мавжуд криптографик калитларни тақсимлаш алгоритми ва протоколларини калит тури, калитни тақсимлаш вазияти, калитларни тақсимлаш усули, калитларни тақсимлаш схемаси ва уларнинг бардошлилигини таъминловчи муаммо тури каби 5 та белги асосида таснифланди.



17-расм. Криптографик калитларни тақсимлаш протоколларининг таснифи

2-БОБ. ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА АСОСЛАНГАН КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИ ВА ПРОТОКОЛЛАРИ

2.1. Эллиптик эгри чизиқлар криптографияси

Кўплаб ошкора калитли криптографик маҳсулотлар ва стандартлар деярли анъанавий мавқега эришган RSA ва Эль Гамал алгоритмларига асосланган [18-20]. Сўнгги вақтларда криптотаҳлил усулларининг ва ҳисоблаш техникасининг кескин ривожланиши тизимларнинг ишончли ҳимояси учун калит битлари сонининг ҳам катта бўлишига олиб келди, бу эса анъанавий тизимларни қўлловчи тизимлар иловасини юкланиш вақтининг ортишига олиб келди. Бу ўз навбатида катта транзакцияларни ҳимоялаш талаб этиладиган, электрон тижоратга ихтисослашган алоқа тугунларида кўплаб муаммоларни келтириб чиқарди. Шу боис анъанавий мавқега эришган тизимларга рақиб бўлган эллиптик эгри чизиқларга асосланган криптография вужудга келди [21-25]. Ҳозирги кунда эллиптик эгри чизиқларнинг криптография соҳасига тадбиқи кенг қўлланилмоқда. Эллиптик эгри чизиқлар назарияси замонавий криптография ва сонлар назариясида асосий ўрганиш объектларидан бири ҳисобланади. Мисол учун, булар Эндрю Уайлс (Ричард Тейлор билан биргаликда) Ферманинг буюк теоремасини исботлашда фойдаланилган.

Эллиптик эгри чизиқлар криптографияси — криптографиянинг мустақил бир бўлими ҳисобланиб, чекли майдонлардаги эллиптик эгри чизиқларга асосланган носимметрик криптотизимларни ўрганади. Эллиптик эгри чизиқлар криптографиясининг асосий афзаллиги ҳозирги кунгача эллиптик эгри чизиқлардаги нуқталар группасини дискрет логарифмлаш масаласи асосида субэкспоненциал алгоритмларни ечишга қаратилган муаммонинг аниқланмаганлиги ҳисобланади.

Криптотизимларни яратишда эллиптик эгри чизиқлардан фойдаланиш бир-биридан мустақил равишда Нил Коблиц ва Виктор Миллерлар томонидан 1985 йилда тавсия этилган.

Носимметрик криптотизимлар криптобардошлиги бир қатор математик масалаларнинг ечиш мураккаблигига асосланган. Илк очиқ калитли криптотизим, яъни алгоритм RSAнинг криптобардошлиги мураккаб

сонларни туб кўпайтувчиларга ажратиш муаммосига асосланганлигидадир. Эллиптик эгри чизиқларда худди шу криптобардошликда RSAга нисбатан калит ўлчами қисқа бўлади, бу маълумотни сақлаш ва узатишда сезиларли даражада сарфнинг камайишига олиб келади.

Мисол учун RSA-2005 конференциясида Миллий хавфсизлик агентлиги “Suite B” ни яратишда фақат эллиптик эгри чизиқли алгоритмлардан фойдаланилганлигини баён қилган.

Шундай қилиб, эллиптик эгри чизиқларга асосланган криптографик тизимларнинг анъанавий тизимларга нисбатан афзаллиги, уларда фойдаланиладиган калит узунлиги разряди кичик бўлганда ҳам, эквивалент ҳимоя билан таъминлашидадир. Бу эса қабул қилувчи ва узатувчи мослама процессорларининг юкланиш вақтини камайтиради.

Эллиптик эгри чизиқлар қуйидаги кўринишдаги тенгламалар ёрдамида берилади:

$$y^2 + axy + by = x^3 + cx^2 + dx + g,$$

бунда a, b, c, d бутун сонлар.

Эллиптик эгри чизиқ O деб белгиланган махсус бўлмаган (чексизликдаги нуқта, нол элемент) элементни ўз ичига олади.

Эллиптик эгри чизиқ таърифидан агар учта нуқта бир тўғри чизиқда ётса, уларнинг йиғиндиси O эканлиги келиб чиқади. Бу таърифдан эллиптик эгри чизиқ нуқталарининг қўшишни қуйидаги қоидалари келиб чиқади:

1. Қўшишда O нол элементи сифатида қатнашади, яъни $O=-O$ бўлиб, эллиптик эгри чизиқнинг ихтиёрий нуқтаси учун $P+O=P$.

2. Вертикал чизиқ эллиптик эгри чизиқни бир хил x абциссали иккита нуқтада кесиб ўтади. Бу чизиқ эгри чизиқни чексизлик нуқтасида ҳам кесиб ўтади. Шунинг учун $P_1+P_2+O=O$ ва $P_1=-P_2$, бунда $P_1=(x,y)$, $P_2=(x,-y)$. “Манфий” ишорали нуқта бу x координатаси худди ўша қийматга, y координатаси эса ишораси бўйича қарама-қарши қийматга эга бўлган нуқтадир.

3. Турли x координатали Q ва R нуқталарни қўшиш учун, бу икки нуқта орқали тўғри чизиқ ўтказилади ва бу тўғри чизиқнинг эллиптик эгри чизиқ билан кесишган учинчи нуқтаси P_1 топилади. Агар бу нуқталарнинг бирортасида тўғри чизиқ эллиптик эгри чизиққа уринма бўлмайдиган бўлса,

у ҳолда бу тўғри чизиқнинг ЭЭЧ билан фақат битта кесишиш нуқтаси топилади. Бунда $Q + R = -P_1$.

4. Q нуқтани иккилантириш учун Q нуқтадан уринма ўтказиш керак ва бошқа S кесишиш нуқтасини топиш керак. Бунда $Q + Q = 2Q = -S$.

Қўшишнинг юқорида келтирилган хоссалари қўшишнинг барча оддий хоссаларига, масалан, коммутативлик ва ассоциативлик қонунларига бўйсунади. Эллиптик эгри чизиқнинг P нуқтасини k сонга кўпайтириш P нуқтанинг k та нусхасининг йиғиндиси шаклида аниқланган. $2P = P + P$, $3P = P + P + P$ ва ҳоказо.

p - туб сонли модуль бўйича эллиптик группа криптографияда алоҳида қизиқиш касб этади. Бундай группа қуйидагича аниқланади. Иккита манфий бўлмаган ва p дан кичик бўлган бутун a ва b сонлар танланади, бунда

$$4a^3 + 27b^2 \bmod p \neq 0$$

шарт бажарилсин, у ҳолда $E_p(a,b)$ p модуль бўйича эллиптик группани билдиради. Бу группанинг элементлари манфий бўлмаган p дан кичик (x,y) сонлар жуфтлиги бўлиб, чексизликдаги O нуқта билан $y^2 \equiv (x^3 + ax + b)(\bmod p)$ шартни қаноатлантиради.

Эллиптик группа учун $(0,0)$ дан (p,p) гача бўлган, квадрати манфий сон бўлмаган p модуль бўйича тенгламани қаноатлантирадиган фақат бутун қийматлар қаралади.

Эллиптик эгри чизиқда нуқтани топиш қуйидаги алгоритм ёрдамида амалга оширилади:

1. x нинг $0 \le x < p$ шартни қаноатлантирувчи ҳар бир қиймати учун $(x^3 + ax + b) \bmod p$ ҳисобланади.

2. Аввалги қадамда ҳосил қилинган ҳар бир қиймат учун бу қийматнинг p модуль бўйича квадрат илдизи мавжудлиги текширилади. Агар квадрат илдиз мавжуд бўлмаса, у ҳолда $E_p(a,b)$ тўпламда x нинг бу қийматига мос нуқта мавжуд эмас. Агар илдиз мавжуд бўлса, у ҳолда y илдиздан чиқаришга мос келувчи (нол бўлмаган ҳолда) иккита қийматга эга бўлади. (x,y) нинг бу қийматлари $E_p(a,b)$ нинг нуқталари бўлади.

$E_p(a,b)$ да қўшиш қоидасини геометрик формулаларга мос ҳолда қуйидагича ёзиш мумкин:

1. $P + O = P$.

2. Агар $P = (x, y)$ бўлса, у ҳолда $P + (x, -y) = O$. *(x,-y)* нуқта *P* нуқтанинг манфий қиймати дейилади ва *(-P)* каби белгиланади. *(x,-y)* нуқта эллиптик эгри чизиқда ётади ва демак, $E_p(a,b)$ га тегишли бўлади.

3. Агар $P = (x_1, y_1)$ ва $Q = (x_2, y_2)$ бўлса, бунда $P \neq Q$, у ҳолда $P + Q = (x_3, y_3)$ қуйидаги қоидалар асосида аниқланади:

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p,$$

$$y_3 \equiv (\lambda\ (x_1 - x_2) - y_1) \bmod p,$$

бунда

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \Rightarrow P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \Rightarrow P = Q \end{cases}.$$

Эллиптик эгри чизиқ нуқталари қўшиш амалига нисбатан коммутатив ва ассоциатив, яъни нуқталар тўплами чексизлик нуқтаси *O* билан бирга абель группасини ташкил қилади.

Хусусияти 2 бўлган майдонлардаги эллиптик эгри чизиқлар икки хил кўринишда қаралади:

- Суперсингуляр эллиптик эгри чизиқ:

$y^2 + ay = x^3 + bx + c$.

- Суперсингуляр бўлмаган эллиптик эгри чизиқ:

$y^2 + axy = x^3 + bx^2 + c$.

Суперсингуляр эллиптик эгри чизиқнинг ўзига хос афзаллиги шундаки, у учун нуқталар тўпламини ҳисоблаш енгил ҳисобланади, суперсингуляр бўлмаган эллиптик эгри чизиқларни нуқталарини топиш бир қанча қийинчиликлар туғдиради. Суперсингуляр эллиптик эгри чизиқ қўлбола ECC-криптотизимларни яратишда жуда қўл келади. Улардан фойдаланиш унчалик мураккаб бўлмаган процедураларни хисоблаш орқали амалга ошириш мумкинлиги билан бошқаларидан ажралиб туради.

Эллиптик криптографияда асосан қуйидаги ЭЭЧ кўринишларидан фойдаланилади:

- $K = F(p)$ майдон устида, бу ерда туб сон $p>3$, ва туб майдон кенгайтмаси $K = F(p^n)$ устида аниқланган *носуперсингуляр ЭЭЧ,*

- $K=F(2^m)$ майдони устида аниқланган *носуперсингуляр ЭЭЧ.*

Криптографияда эллиптик эгри чизиқдан фойдаланишда барча қатнашувчилар эллиптик эгри чизиқни қуриш учун керак бўладиган барча параметрлар тўпламини келишиб олиши лозим. Эллиптик эгри чизиқ a ва b константалар билан аниқланади: $E: \quad y^2 = x^3 + Ax + B \pmod p$, Кофактор $h = \frac{|E|}{n}$, бу ерда n — G даги нуқталарнинг тартиби, у унча катта бўлиши муҳим эмас ($h \le 4$, одатда $h = 1$ олинади).

Демак, хусусияти 2 бўлган майдон майдон параметрлари тўплами: (m, f, a, b, G, n, h), $\mathbb{Z}_p$ чекли майдон учун (бу ерда $p > 3$) эса (p, a, b, G, n, h).

Бир қанча параметрлар тўплами учун тавсиялар мавжуд:

- NIST (Стандартлар ва тенологиялар миллий институти).
- SECG

Хусусий параметрлар тўпламини яратиш учун қуйидагиларни амалга ошириш зарур:

1. Параметрлар тўпламини танлаш.
2. Шу параметрлар тўпламини қаноатлантирадиган эллиптик эгри чизиқни топиш.

Берилган параметрлар бўйича эллиптик эгри чизиқни аниқлашда қуйидаги икки хил усулдан фойдаланилади:

- Ихтиёрий эллиптик эгри чизиқни танлаш ва нуқталарни аниқлаш алгоритмларидан фойдаланиш.
- Нуқталарни танлаш ва шу асосида кўпайтириш техникасидан фойдаланиб эллиптик эгри чизиқни қуриш.

Бир қанча криптографик ”кучсиз” параметрлар тўплами мавжуд. Улардан фойдаланиш тавсия этилмайди, булар қуйидагилар:

- $\mathbb{F}_{2^m}$ устидаги эллиптик эгри чизиқлар, бу ерда m – туб бўлмаган сон. Бундай эгри чизиқлар билан шифрлаш Вейл атакалари билан тасдиқланган.
- $|E(\mathbb{F}_q)| = q$ ли эллиптик эгри чизиқлар ҳужумларга бардошли эмас. Бундай нуқталар $\mathbb{F}_q$ майдоннинг аддитивлик группасини намоён қилади.

p модуль асосида бўлиш (кўпайтириш ва қўшиш жараёни учун керак)да, агар p га 2 ни даражасидаги туб сонлар олинса, тезроқ ишлаши мумкин. p Мерсен туб сонларини ишлатиш ҳам мумкин. Мисол учун, $p = 2^{251} - 1$ ёки $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ лар яхши танлов ҳисобланади. Стандартлар ва тенологиялар миллий институти p учун туб сонларни қўллашни тавсия этади.

Эллиптик эгри чизиқларнинг яна бир ютуқларидан бири NIST тавсия этишича $a = -3$ ни танлаш Якоби координталарида қўшиш жараёнини анча тезлаштиради.

NIST 15 та эллиптик эгри чизиқни тавсия этади. FIPS-186-3 (маълумотларни қайта ишлаш бўйича федерал стандарт) эса тавсиясига асосан 10 та чекли майдонларни ишлатишни тавсия этади. Шулардан бир нечтаси қуйидагилар:

- $\mathbb{F}_p$ майдон, бу ерда p нинг узунлиги 192, 224, 256, 384 ёки 521 бит.
- $\mathbb{F}_{2^m}$ майдон, бу ерда m = 163, 233, 283, 409 ёки 571 бит.

Ҳар бир чекли майдон учун битта эллиптик эри чизиқ тавсия этилади. Бу чекли майдонлар ва эгри чизиқлар юқори криптобардошлик ҳамда дастурий таъминот ишлаб чиқишда самарадорлиги сабабли танлаб олинган.

Хусусан олганда эллиптик эгри чизиқлар электрон рақамли имзо стандартлари (ГОСТ Р 34.10-2001, ECDSA), калитларни тақсимлаш алгоритмлари (ECDH, ECMO ва ECMQV), сонларни тубликка текшириш, факторлаш алгоритмлари (Ленстри алгоритми) ва бошқа кўплаб ҳолатларда ишлатилади.

2.2. Диффи–Хеллманнинг ECDH калитларни тақсимлаш алгоритми

Диффи-Хеллманнинг эллиптик эгри чизиқларга асосланган аналоги ECDH қуйидаги кўринишда бўлади: аввал катта туб p сон ва ЭЭЧ учун a, b параметрлар танланади [20, 25-26]. Бу эллиптик нуқталар группаси $E_p(a, b)$ ни беради. Сўнгра $E_p(a, b)$ да генерацияловчи нуқта $G=(x,y)$ танланади. G ни танлаганда $nG=0$ шартни қаноатлантирувчи n нинг энг кичик қиймати жуда ҳам катта туб сон бўлиши муҳим. Криптотизимнинг G ва $E_p(a, b)$ параметрлари барча иштирокчиларга маълум параметр ҳисобланади.

A ва **B** иштирокчилар орасидаги калит тақсимоти қуйидаги схема бўйича амалга оширилади:

1. **A** иштирокчи бутун $n_A < n$ сонни танлайди. Бу сон **A** иштирокчининг махфий калити бўлади. Сўнгра **A** иштирокчи очиқ калити $P_A = G \times n_A$ генерация қилади. Очиқ калит $E_p(a, b)$ га тегишли нуқта бўлади.

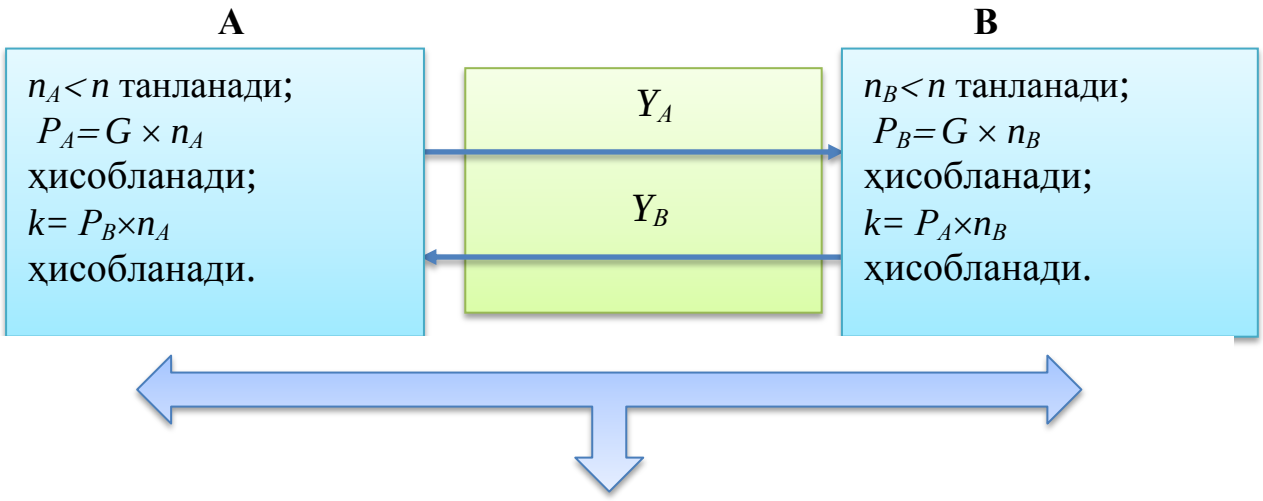
2. **B** иштирокчи ҳам худди шундай n_B махфий калитни танлайди ва $P_B = G \times n_B$ очиқ калитни ҳисоблайди.

3. **A** иштирокчи $k = P_B \times n_A$ махфий калитни, **B** иштирокчи эса $k = P_A \times n_B$ махфий калитни генерация қилади.

3-қадамдаги иккала формула ҳам бир хил қийматни беради

$$P_B \times n_A = (G \times n_B) \times n_A = (G \times n_A) \times n_B = P_A \times n_B.$$

Бу схемани бузиши учун бузғунчи G ва G k нинг қийматларидан k ни ҳисоблаб топиши керак бўлади (18-расм). Бу эса қийин ечиладиган масала ҳисобланади.



18-расм. ЭЭЧларга асосланган Диффи- Хеллман схемасининг аналоги

Модуль $p=211$ ва эллиптик нуқталар тўплами $E_{211}(0,-4)$ ни танлаймиз. Уларга мос келувчи ЭЭЧ $y^2 = x^3 - 4$ ва $G=(2,2)$. Ҳисоблашлар $241\,G = 0$ эканини кўрсатади. **A** иштирокчининг махфий калити $n_A = 121$ бўлсин, у ҳолда **A** иштирокчининг очиқ калити $P_A = 121(2,2) = (115,48)$ бўлади. **B** иштирокчининг махфий калити $n_B = 203$ бўлсин, у ҳолда **B** иштирокчининг

очиқ калити $P_B = 203(2,2) = (130,203)$ бўлади. У ҳолда умумий махфий калит 121(130,203)=203(115,48)=(161,169) бўлади.

ЭЭЧларга асосланган криптографияда махфий калит сифатида сонлар жуфтлиги қаралади. Агар бу калитдан анъанавий шифрлашда фойдаланилмоқчи бўлса, у ҳолда бу иккита сондан мос битта қиймат генерация қилинади. Ёки бўлмаса *x* ё *y* координаталардан бирини ишлатиш мумкин.

2.3. Эллиптик эгри чизиқли MQV калитларни тақсимлаш алгоритми

MQV (Менезес-Кью-Ванстоун) калитларни тақсимлаш протоколи бўлиб, Диффи-Хеллман алгоритми базасида қурилган. Протокол каноник чекли майдонлар учун ҳам ишлаши мумкин, хусусий ҳолда эллиптик эгри чизиқларга асоланган ECMQV алгоритми мавжуд.

MQV алгоритми биринчи марта Алфред Менезис, Кью, Скотт Ванстоунлар томонидан 1985 йилда тавсия этилган. 1998 йилда эса унинг модификацияланган варианти ишлаб чиқилган. Алгоритмнинг бир, икки ва уч ўтишли турлари мавжуд. MQV алгоритми очиқ калитли криптотизимлар бўйича IEEE P1363 стандартига киритилган.

MQV алгоритмининг бир нечта турлари учун олинган патентлар Certicom компаниясига тегишли ҳисобланади. MQV алгоритмининг бир қанча камчиликлари 2005 йилда такомиллаштирилган HMQV алгоритмида бартараф этилган.

Келтирилган иккала MQV ва HMQV алгоритмлар бир қатор заифликларга эга бўлиб, бу камчиликлар FHMQV протоколида бартараф этилган. Криптобардошлигини ошириш, алгоритм ва калит узунлигига бўлган сарф-ҳаражатларни пасайтириш учун эллиптик эгри чизиқларга асосланган ECMQV алгоритми таклиф этилган.

ECMQV алгоритмининг тавсифи қуйидагича баён этилади:

А иштирокчида статик калитлар жуфтлиги (W_a, w_a)лар мавжуд, бу ерда W_a унинг очиқ калити ва w_a унинг ёпиқ калити. **В** иштирокчида статик калитлар жуфтлиги (W_b, w_b) лар мавжуд, бу ерда W_b унинг очиқ калити ва w_b унинг ёпиқ калити ҳисобланади. $\bar{R}$ ни аниқлаймиз. $R = (x, y)$ эллиптик эгри чизиқдаги нуқта бўлсин.

Унда $\bar{R} = (x \bmod 2^L) + 2^L$ бўлади, бу ерда $L = \left\lceil \frac{\lfloor \log_2 n \rfloor + 1}{2} \right\rceil$ га тенг ва n эса P генератордаги тартиби ҳисобланади. Бундан ташқари кофактор h ни ҳам аниқлаймиз $h = \frac{|G|}{n}$, бу ерда $|G|$ G группанинг тартиби ҳисобланади ва техник жиҳатдан қуйидаги тенгликни қаноатлантириши керак (3-жадвал): $gcd(n, h) = 1$.

3-жадвал

ECMQV алгоритмининг бажарилиш жараёни

Қадам	**Жараён**
1	**A** иштирокчи (R_a, r_a) калитлар группасини ҳосил қилади, r_a ни ихтиёрий генерация қилади ва $R_a = r_a P$ ни ҳисоблайди. Бу ерда P — эллиптик эгри чизиқдаги нуқта. Шундан сўнг **B** иштирокчига вақтинчалик очиқ калит R_a ни жўнатади.
2	**B** иштирокчи (R_b, r_b) калитлар группасини ҳосил қилади, r_b ни ихтиёрий генерация қилади ва $R_b = r_b P$ ни ҳисоблайди. Шундан сўнг **A** иштирокчига вақтинчалик очиқ калит R_b ни жўнатади
3	**A** иштирокчи R_b вақтинчалик очиқ калитни G группага тегишлилигини текширади, ундан ташқари R_b нол элемент эмаслигига ҳам текширади. Шундан сўнг группа элементи Kab ни ҳисоблайди, $Kab = hs_a S_b$, бу ерда $s_a = (r_a + \bar{R}_a w_a) mod n$ ва $S_b = R_b + \bar{R}_b W_b$. Агар $Kab = O$ бўлса **A** иштирокчи **B** иштирокчи дан келган маълумотларни бекор қилади. Акс ҳолда натижани умумий махфий калит сифатида қабул қилади.
4	**B** иштирокчи R_a вақтинчалик очиқ калитни G группага тегишлилигини текширади, ундан ташқари R_a нол элемент эмаслигига ҳам текширади. Шундан сўнг группа элементи Kba ни ҳисоблайди, $Kba = hs_b S_a$, бу ерда $s_a = (r_a + \bar{R}_a w_a) mod n$ ва $S_b = R_b + \bar{R}_b W_b$. Агар $Kba = O$ бўлса **A** иштирокчи **A** иштирокчи дан келган малумотларни бекор

	қилади. Акс ҳолда натижани умумий махфий калит сифатида қабул қилади.

Асосий протокол қуйидаги сабабларга кўра ажойиб ечим ҳисобланади:

1. У калит ошкора бўлмаган тарзда идентификация қилади ва ҳар бир шерик учун навбатдаги ҳимоя ҳосил қилинади.

2. Фақат хисоблаш жараёнида самарали бўлмай, балки ўтказиш қобилиятидан ҳам ютуққа эришади. Бундан ташқари жараёнлар фақат майдонларда ва оддий ҳолда амалга оширилади. Ҳар бир фойдаланувчи учун 2.5 та ҳисоблаш (қўпол баҳолаганда) бажарилади, яни биттаси вақтинчалик калит жуфтлигини ҳосил қилиш бўлса, қолгани s_a ёки s_b скаляр кўпайтириш учун.

B иштирокчининг ҳисоблашлари:

$$Kba = h \cdot s_b(R_a + \bar{R}_a W_a) = h \cdot s_b(r_a P + \bar{R}_a w_a P) = h \cdot s_b(r_a + \bar{R}_a w_a)P = h \cdot s_b s_a P$$

A иштирокчининг ҳисоблашлари:

$$Kab = h \cdot s_a(R_b + \bar{R}_b W_b) = h \cdot s_a(r_b P + \bar{R}_b w_b P) = h \cdot s_a(r_b + \bar{R}_b w_b)P = h \cdot s_b s_a P$$

Шунинг учун ҳам $Kab = Kba$ га ҳақиқатдан тенг ва $K = h \cdot s_b s_a P$ калитга эквивалент ҳисобланади.

2.4. Эллиптик эгри чизиқли Месси-Омар калитларни тақсимлаш алгоритми

Фараз қилайлик *E* - *n* тартибли ЭЭЧ, *e* эса *(e, n)= 1, 1<e<n* шартни қаноатлантирувчи сон. Инвертлаш алгоритмидан фойдаланиб $d \equiv e^{-1} \bmod n$ ни топамиз. Бутун сонлар устидаги модуль арифметикаси қонунлари билан ЭЭЧ нуқталари устидаги модуль арифметикаси қонунлари бир хил бўлгани учун, ЭЭЧнинг ихтиёрий *P* нуқтасини қуйидаги формулалар ёрдамида ҳисоблаш мумкин:

$$Q = eP,$$

$$R = dQ.$$

Месси – Омур протоколи ЭЭЧнинг берилган нуқтасини базавий нуқтага нисбатан скаляр кўпайтувчисини аниқлаш муаммосининг ечилишига, яъни ЭЭЧларда дискрет логарифм масаласини ечишга асосланган [10-12].

A ва **B** иштирокчилар орасида калит тақсимотини қуйидаги схема ёрдамида амалга оширилади (19-расм):

1. **A** иштирокчи $e_A < n$ бутун сонни танлайди ва $d_A \equiv e^{-1}{}_A \bmod n$ ни ҳисоблайди. e_A сон **A** иштирокчининг махфий калити бўлади. d_A эса **A** иштирокчининг шахсий шифрни очиш калити бўлади. Сўнгра **A** иштирокчи ўзининг m хабарини P_m ЭЭЧнинг бирор нуқтасига жойлаштиради ва ўзининг махфий e_A га кўпайтириб, (очиқ калит генерация қилади): яъни

$$P_A = e_A P_m$$ нуқтани ҳосил қилади.

2. **B** иштирокчи ҳам ўзи учун худди шундай шахсий шифрлаш ва шифрни очиш калитлари e_B ва d_B калитларни ҳосил қилади. Сўнгра **B** иштирокчи ўзининг махфий калити қийматини **A** иштирокчининг ошкора P_A калитига кўпайтириб (ошкора калитни генерация қилади): яъни

$$P_B = e_B P_A$$

нуқтани ҳосил қилади.

3. Бу қийматни **A** иштирокчига жўнатади.

4. **A** иштирокчи

$$P_O = d_A P_B$$ ни ҳисоблайди.

5. Ҳисоблаб топилган қийматни **B** иштирокчига юборади.

6. **B** иштирокчи юборилган қийматни ўзининг махфий шифрни очиш калитига d_B кўпайтириб, **A** иштирокчининг m хабарига мос P_m нуқтани топади:

$$P_m = d_B P_O .$$

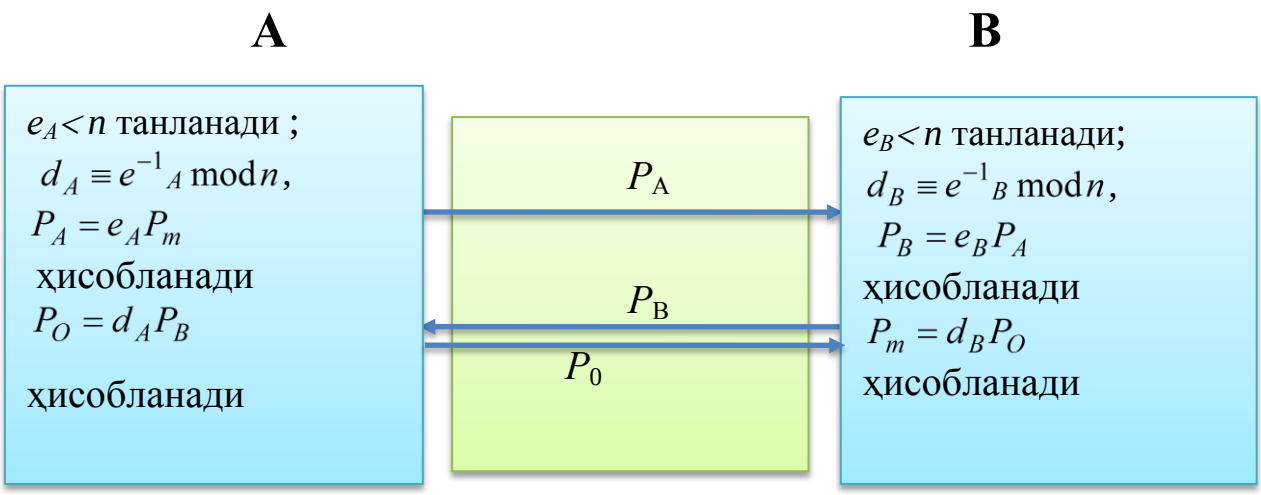
P_O ни ҳисоблаб **A** иштирокчи ўзининг шифрлаш калитининг фаолиятини бартараф қилади:

$$P_O = d_A P_B = d_A(e_B P_A) = d_A(e_B(e_A P_m)) = e_B(d_A(e_A P_m)) = e_B P_m .$$

Демак, **B** иштирокчи қуйидагини олади:

$$d_B P_O = d_B(d_A P_m) = P_m .$$

m хабар анъанавий криптотизимлар учун калит ўрнида ишлатилиши мумкин. Бу ҳолда ЭЭЧнинг ўзидан бошқа протокол параметрлари тўғрисида ҳеч қандай ахборотни эълон қилиш талаб этилмайди. Бунинг эвазига очиқ канал бўйлаб уч марта узатиш амалга оширилади.



19-расм. Месси – Омур схемаси бўйича калит тақсимлаш протоколи

2.5. Эллиптик эгри чизиқли криптотизимлар учун Эль Гамал калитларни тақсимлаш алгоритми

RSA криптотизимида Эль Гамал протоколининг қўлланилиши қуйидагича бўлади. n туб сон ва ихтиёрий $p < n$ ва $q < n$ сонлар танланади. Очиқ калит сифатида $(n, p, p^q \bmod n = y)$ учлик, махфий калит сифатида эса q дан фойдаланилади.

Очиқ m матнни шифрлаш учун $a \equiv p^k (\bmod n), b(m) \equiv (y^k m)(\bmod n)$ ҳисоблаш керак бўлади, бунда k - ихтиёрий n билан ўзаро туб бўлган сон. $a, b(m)$ жуфтлик шифрматн бўлади. Равшанки, матнни шифрини очиш учун $m = (b(m) / a^q) \bmod n$ ҳисобланади.

ЭЭЧнинг мультипликатив группасини қўлловчи Эль Гамал протоколининг модификацияси қуйидагича:

Фараз қилайлик, M очиқ матн E ЭЭЧнинг нуқтаси бўлсин. Агар очиқ матн бир қанча нуқталар тўпламидан иборат бўлса, қуйида келтириладиган алмаштиришлар ҳар бир нуқта учун алоҳида бажарилади.

Криптотизимнинг **А** ва **В** иштирокчилари Диффи-Хеллман протоколи бўйича $k_A Q$ ва $k_B Q$ калит қисмларини алмаштиришди. **А** иштирокчи **В** иштирокчига M хабарни юбормоқчи бўлса, l махфий сонни танлайди ва **В** иштирокчига ЭЭЧнинг $E = (lQ, M + l(k_B Q))$ нуқталар жуфтини юборади.

Олинган ахборотни шифрини очиш учун **B** иштирокчи $T = k_B(lQ)(l(k_BQ))$ ни ҳисоблаши керак. Бунда $M = M + l(k_BQ) - T$.

Эътиборли жиҳати шундаки, lQ нуқта шифрни йиғиш функциясини бажаради ва демак, бирон бир Q нуқта икки марта ишлатилиши мумкин эмас. Агар икки марта ишлатилса, икки хил шифрматнни таққослаш натижасида нафақат шифрматннинг шифрини синдириш, балки тизимнинг махфий компоненталарини аниқлашнинг ҳам имкони туғилади.

2.6. Модуль арифметикасига асосланган протоколлар

Модуль арифметикасига асосланган калитларни тақсимлаш протоколи ҳар иккала томондан симметрик бажараладиган уч босқичдан иборат [1-5].

Биринчи босқичда **A** ва **B** иштирокчилар ўзининг махфий k_A, d_A ҳамда k_B, d_B маълумотларидан фойдаланиб, қуйидагиларни ҳисоблайди:

$$s_A = (k_A + x_A a_A d_A) \bmod n,$$
$$s_B = (k_B + x_B a_B d_B) \bmod n.$$

Иккинчи босқичда улар эллиптик эгри чизиқнинг нуқталарини ҳисоблашади:

$$U_A = R_B + x_B a_B Q_B,$$
$$U_B = R_A + x_A a_A Q_A.$$

Учинчи босқичда улар эллиптик эгри чизиқ нуқтасини ҳисоблашади:

$$W = s_A U_A,$$
$$W = s_B U_B.$$

Чап тарафидаги белгилашнинг бир хиллиги бу иккала тенгликнинг қиймати тенглигини билдиради. Буни эса қуйидагича исботлаш мумкин.

A иштирокчи учун

$$s_A U_A = ((k_A + x_A a_A d_A) \bmod n)(R_B + x_B a_B Q_B) =$$
$$= ((k_A + x_A a_A d_A) \bmod n)(k_B P + x_B a_B d_B P) =$$
$$= ((k_A + x_A a_A d_A) \bmod n)(k_B + x_B a_B d_B) P =$$
$$= ((k_A + x_A a_A d_A)(k_B + x_B a_B d_B) \bmod n) * P.$$

B иштирокчи учун

$$s_B U_B = ((k_B + x_B a_B d_B) \bmod n)(R_A + x_A a_A Q_A) =$$

$$= ((k_B + x_B a_B d_B) \bmod n)(k_A P + x_A a_A d_A P) =$$
$$= ((k_B + x_B a_B d_B) \bmod n)(k_A + x_A a_A d_A) P =$$
$$= ((k_B + x_B a_B d_B)(k_A + x_A a_A d_A) \bmod n) * P .$$

Қараб чиқилаётган протоколнинг талқинида модуль арифметикаси эллиптик эгри чизиқлар арифметикаси билан уйғунлаштирилган.

Модуль арифметикасидан фойдаланилмаган ва s_A, s_B сонлар аввалдан ҳисобланмаган ҳолдаги талқинни кўриб чиқамиз.

A иштирокчи Q_B нуқтани a_B константага ва x_B константага кўпайтириб, сўнгра ҳосил бўлган нуқтани R_B нуқта билан қўшиб эллиптик эгри чизиқнинг U_A нуқтасини ҳисоблаб топиши мумкин. Худди шундай B иштирокчи ҳам U_B нуқтани ҳисоблаб топиши мумкин.

W нуқтани олиш учун **A** ва **B** иштирокчилар олинган нуқталарни s_A, s_B константаларга кўпайтириш лозимлигини кўзда тутган ҳолда, қуйидаги алгоритм бўйича амалга оширишлари мумкин (**A** иштирокчи учун):

1) Эллиптик эгри чизиқ нуқтасини константага кўпайтириш натижасида $k_A U_A$ ни ҳисоблаш.

2) Мос катталикларни кетма-кет кўпайтириш йўли билан $x_A(a_A(d_A U_A))$ ни аниқлаш.

3) 1) ва 2) пунктларда топилган эллиптик эгри чизиқнинг иккита нуқтаси қўшилади.

Протокол тугалланишида **A** ва **B** иштирокчилар анъанавий шифрлаш тизимларида координаталари махфий калитнинг бинар кодини қурувчиси сифатида қўлланилиши мумкин бўлган эллиптик эгри чизиқнинг махфий W нуқтасига эга бўладилар.

2.7. Эллиптик эгри чизиқларга асосланган протоколларнинг криптографик бардошлилиги

Криптографик бардошлик (бардошлик) деб – криптографик тизимнинг ҳужумларга қарши тура олиш қобилиятига айтилади [9-11]. Миқдорий жиҳатдан криптобардошлик етарли эҳтимоллик билан криптотаҳлилчини муваффақиятга элтадиган энг яхши криптотаҳлил алгоритмининг

мураккаблиги билан ўлчанади.

Махфий калит асосан модуль узунлиги билан аниқлангани сабабли мавжуд калит тақсимоти алгоритмларининг бардошлигини ошириш модулнинг бинар узунлигини ошириш асосида амалга оширилади.

Ушбу бобда келтирилган калит тақсимлаш алгоритмларининг криптобардошлиги уларни кўпчилик томонидан жуда мураккаб деб тан олинган масала - эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблигига асосланган.

Чекли майдон устидаги ЭЭЧ нуқталари группасида икки нуқтанинг йиғиндиси амали аниқланган бўлсин, яъни $mP = \underbrace{P + P + ... + P}_{m}$. ЭЭЧда дискрет логарифмлаш масаласини ечиш, бу шундай натурал m сон керакки, берилган A ва P нуқталар учун $mP = A$ тенглик ўринли бўлсин.

ЭЭЧда дискрет логарифмлаш масаласи қийин ечиладиган муаммолардан бири бўлиб, бу масаланинг ечиш алгоритмларининг мураккаблиги [21, 22, 24-28] икки хил бўлади: экспоненциал мураккабликдаги N^{λ} алгоритмлар ва субэкспоненциал мураккабликдаги $L_N(\alpha, c) := O(\exp(\lambda(\log N)^{\alpha}(\log\log N)^{1-\alpha}))$ алгоритмлар, бунда N - киритиладиган сон, $0 < \alpha < 1$ ва λ– константалар.

Шенкс усулидан фойдаланиб, ихтиёрий чекли циклик группада ЭЭЧ дискрет логарифмлаш муаммосини $\sqrt{n}$ амал ёрдамида ечиш мумкин. Бу усулда иккита $t = \sqrt{n}$ ўлчамли рўйхат тузилади. Биринчи жадвал $\{(i, itP),\ i = 0,..,t-1\}$ жуфтликлардан иборат бўлиб, иккинчи элементи бўйича сараланган бўлади. Иккинчи жадвал $\{(j, Q + jP),\ j = 0,..,t-1\}$ жуфтликлардан иборат бўлиб, улар ҳам иккинчи элементи бўйича сараланган. Бундай сараланган жадвалда иккинчи элементи бўйича тенг бўлган иккита жуфтликни топиш осон, яъни (i, itP) ва $(j, Q + jP)$ бўлиб, бунда $itP = Q + jP$. У ҳолда n модуль бўйича $k = it - j$. Аммо бу усулни тадбиқ этишда жадвалларни сақлаш учун етарлича катта хотира талаб қилинади.

ЭЭЧда дискрет логарифмлаш масаласини ечишниг маълум усулларидан энг машҳури Поллардниng ρ- ва λ- усулларидир [1, 40]. ЭЭЧ нуқталарини қўшиш билан аниқланувчи Поллардниng ρ-усули мураккаблигини қуйидаги ифода орқали баҳолаш мумкин:

$$I_p = \sqrt{\frac{\pi q}{2}},$$

бу ерда q – ЭЭЧ базавий нуқталари тартиби.

[40]да Поллард ρ-усули тезлигини $\sqrt{2}$ мартага ошириш мумкинлиги кўрсатилган. У ҳолда усул мураккаблиги $I_p = \sqrt{\frac{\pi q}{4}}$ билан баҳоланади.

Поллард ρ-усулининг афзаллик томонларидан бири криптотаҳлил жараёнини мустақил бир нечта параллел жараёнларга ажратишдир. Бу ҳолда ҳар бир жараённи амалга ошириш мураккаблиги $I_p = \sqrt{\frac{\pi q}{2r^2}}$ ва $I_p = \sqrt{\frac{\pi q}{4r^2}}$ билан баҳоланади.

Поллардниng ρ-усулида мураккаблиги баҳоси модуль узунлигига боғлиқ бўлиб, 4-жадвалда бунга доир маълумотлар келтирилган.

4-жадвал

Мураккаблик баҳосининг модуль узунлигига боғлиги

Базавий нуқталари тартиби q	**ρ- Поллард усули мураккаблиги I_ρ**
2^{128}	$2^{64,72}$
2^{160}	$2^{80,17}$
2^{256}	$2^{128,31}$
2^{512}	$2^{256,30}$
2^{1024}	$2^{512,26}$

ЭЭЧда дискрет логарифмлаш масаласини Поллард ρ-усулидан фойдаланиб ечиш мураккаблигига тааллуқли келтирилган маълумотлар шуни кўрсатадики, калит тақсимлаш алгоритмларининг бардошлигини оширишнинг ҳозирги кундаги энг самарали усули ЭЭЧ базавий нуқталари тартиби q ни ошириш усулидир.

Поллард λ-усули мураккаблиги $I_\lambda=2\sqrt{q}$ билан ва параллеллашда $I_\lambda=2r^{-1}\sqrt{q}$ билан баҳоланади.

Поллардннг иккала усулининг қиёсий таҳлили Поллард λ-усули Поллард ρ-усулига нисбатан мураккаброқлигини кўрсатади.

2004 йилда Поллард параллелланган алгоритми асосида “бузилган” ЭЭЧ калитининг энг катта узунлиги *109* битни ташкил этди [46].

ЭЭЧда дискрет логарифмлаш масаласини Поллард ρ-усулидан фойдаланиб ечиш мураккаблигига тааллуқли келтирилган маълумотлар шуни кўрсатадики, ЭРИ алгоритмларида базавий нуқтаси $q\geq 2^{256}$ тартибли ЭЭЧ қўлланиши ЭЭЧ базасидаги ЭРИ зарур бардошлигининг келажакдаги истиқболини таъминлайди. Бу ГОСТ Р 34.10-2001нинг 10 йил давомида муваффақиятли эксплуатацияси ва калитни очиш мураккаблиги $3*10^{38}$ арифметик амалдан иборатлиги билан ҳам асосланади.

Аммо ЭЭЧда субэкспоненциал алгоритмларни яратиш учун бўлган барча уринишлар муваффақиятсизликка учради, бунинг эса жиддий сабаби мавжуд. Субэкспоненциал мураккабликка эга алгоритмларни яратишда берилган группа ҳалқага жойланади, унда эса кичкина туб элементлар кўп. Масалан, дискрет логарифмни содда майдоннинг мультипликатив группасида ҳисоблашнинг субэкспоненциал алгоритмида ихтиёрий бутун сонни катта эҳтимоллик билан унча катта бўлмаган туб кўпайтувчиларга ёйиш мумкинлиги ҳақидаги хоссадан фойдаланилади. Шундай хоссага бутун алгебраик сонлар ҳам эга бўлиб, бунда туб бутун алгебраик сонларнинг катта тўплами мавжуд. Худди шунингдек чекли майдон устида аниқланган кўпҳадларнинг ҳалқаси ҳам шундай хусусиятга эга, чунки у ерда ҳам

кичкина тартибли келтирилмайдиган кўпҳадлар етарли. Аммо ЭЭЧ ларда бундай хусусиятга эга бўлган нуқталар йўқ. Бу фактни Н.Коблиц эллиптик криптографияни сақловчи тилла қалқон деб атаган. ЭЭЧ нуқталарининг ўзида дискрет логарифмлашнинг субэкспоненциал алгоритми мавжуд бўлмаса ҳам, келажакда ҳам бўлиш эҳтимоллиги жуда кам бўлгани билан, хар доим берилган дискрет логарифмлаш масаласини субэкспоненциал алгоритмлар мавжуд бўлган бошқа группалардаги шунга ўхшаш масалага ўтказиш имконияти мавжуд.

Биринчи шундай ўтказиш 1963 йилда А.Менезес, Т.Окамото ва С.Вэнстон [27] томонидан Вейлни қўшиш ёрдамида амалга оширилган бўлиб, бунда $GF(2^m)$ майдон устидаги берилган масала $GF(2^{km})$кенгайтмали мультипликатив группадаги дискрет логарифмлаш масаласига келтирилган. Агар кенгайтманинг даражаси k кичик бўлса, у ҳолда берилган дискрет логарифмлаш масаласи учун субэкспоненциал алгоритм мавжуд бўлади. Ҳисоблаш нуқтаи назаридан $k \le 6$ бўлгандаги суперсингуляр чизиқларни криптографияда қўллашдан воз кечишди. Менезес-Окамото-Вэнстон томонидан таклиф этилган шарт ёрдамида бизни қизиқтирадиган майдонлар диапазонида ихтиёрий берилган k учун эгри чизиқ танлаш мумкин, бунда $k > 30$ бўлиши етарли. Бу шартни ихтиёрий майдон устидаги кўпгина ЭЭЧ да дискрет логарифмлаш масаласи субэкспоненциалга келтирилмаслиги ва бу ҳолат ҳар бир чизиқ учун алоҳида бажарилиши маъносида локал дейилади.

Келтирилганлардан хулоса қилиб шуни айтиш мумкинки, криптографик алгоритмларни қуриш учун мўлжалланган ЭЭЧ қуйидаги шартларни қаноатлантириши керак:

– ЭЭЧ циклик группасининг тартиби n туб сон бўлиши лозим, Полиг-Хеллман усулини қўллашдан бошқа ҳолларда.

– Экспоненциал мураккаблик усулининг параллеллаш имконини олдини олиш учун ЭЭЧ циклик группасининг тартиби n етарлича катта бўлиши керак. Ҳисоблаш техникасининг яқин 5-10 йилдаги ривожланишини эътиборга олиб, n тартиб 2^{160} дан кам бўлмаслиги лозим.

– ЭЭЧ циклик группасининг тартиби n бу циклик группадаги дискрет логарифмлаш масаласини берилган майдондаги кенгайтириш тартиби 30 дан кичик бўлган мультипликатив группадаги дискрет логарифмлаш масаласига келитиришнинг олдини олиш учун Менезес-Окамото-Вэнстон шартини қаноатлантириши керак.

Қуйидаги 5-жадвалда эллиптик эгри чизиқларга асосланган калитларни тақсимлаш протоколларига қилинадиган ҳужум турлари кўрсатилган.

5-жадвал

Ҳужумларнинг эллиптик эгри чизиқларга асосланган калитларни тақсимлаш протоколларига таъсири

№	Протокол номи	Ҳужум турлари
1	**Диффи –Хеллманнинг ECDH калитларни тақсимлаш алгоритми**	Иштирокчилар ўртасида ўзаро идентификация таъминланмайди
2	**Эллиптик эгри чизиқли MQV калитларни тақсимлаш алгоритми**	**B** иштирокчи калитни ким томонидан юборилганини билмайди Криптотаҳлилчи бу калитни маълум вақтдан сўнг қайта узатиши мумкин Арбитр маълумотни кимдан келганини ва кимга юбориш кераклиги ҳақида ҳеч нарса билмайди **A** иштирокчи маълумотни арбитрдан келганига тўла ишонч ҳосил қилмайди
3	**Эллиптик эгри чизиқли Месси-Омар калитларни тақсимлаш алгоритми**	Криптотаҳлилчи бу калитни маълум вақтдан сўнг қайта узатиши мумкин **B** иштирокчи калитни ким томонидан юборилганини билмайди
4	**Эллиптик эгри чизиқли криптотизимлар учун Эль Гамал калитларни тақсимлаш алгоритми**	Криптотаҳлилчи маълумотни **B** иштирокчига такроран узатиши мумкин Иштирокчилар маълумотни кимдан келганини билмайди

5	**Модуль арифметикасига асосланган протоколлар**	**А** иштирокчи маълумотни арбитрдан келганига тўла ишонч ҳосил қилмайди Арбитр маълумотни кимдан келганини ва кимга юбориш кераклиги ҳақида ҳеч нарса билмайди

Шундай қилиб, эллиптик эгри чизиқларга асосланган калитларни тақсимлаш протоколларидан фойдаланилаётганда протоколларга қилинаётган ҳужумларни албатта инобатга олиш талаб этилади.

2-боб бўйича хулосалар

1. Ҳозирги кунда ишлаб чиқилган элиптик эгри чизиқлардан фойдаланишга асосланган калитларни тақсимлаш тизимларининг анъанавий тизимларга нисбатан афзаллиги, уларда фойдаланиладиган калит узунлиги разряди кичик бўлганда ҳам, эквивалент ҳимоя билан таъминлашидадир. Бу эса қабул қилувчи ва узатувчи мослама процессорларининг юкланиш вақтини камайтиради.

2. Эллиптик криптографияда асосан қуйидаги ЭЭЧ кўринишларидан фойдаланилади:

- $K = F(p)$ майдон устида, бу ерда туб сон $p>3$, ва туб майдон кенгайтмаси $K = F(p^n)$ устида аниқланган *носуперсингуляр ЭЭЧ,*

- $K = F(2^m)$ майдони устида аниқланган *носуперсингуляр ЭЭЧ.*

3. Криптографияда эллиптик эгри чизиқдан фойдаланишда барча қатнашувчилар эллиптик эгри чизиқни қуриш учун керак бўладиган барча параметрлар тўпламини келишиб олиши лозим. Бир қанча криптографик ”кучсиз” параметрлар тўплами мавжуд. Улардан фойдаланиш тавсия этилмайди. Стандартлар ва тенологиялар миллий институти p учун туб сонларни қўллашни тавсия этади.

4. Махфий калит асосан модуль узунлиги билан аниқлангани сабабли мавжуд калит тақсимоти алгоритмларининг бардошлигини ошириш модулнинг бинар узунлигини ошириш асосида амалга оширилади.

5. Эллиптик эгри чизиқли калит тақсимлаш алгоритмларининг криптобардошлиги уларни кўпчилик томонидан жуда мураккаб деб тан олинган масала - эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблигига асосланган.

6. ЭЭЧда дискрет логарифмлаш масаласини Поллард ρ-усулидан фойдаланиб ечиш мураккаблигига тааллуқли келтирилган маълумотлар шуни кўрсатадики, калит тақсимлаш алгоритмларининг бардошлигини оширишнинг ҳозирги кундаги энг самарали усули ЭЭЧ базавий нуқталари тартиби q ни ошириш усулидир.

7. Калитларни тақсимлаш протоколларидан фойдаланилаётганда протоколларга қилинаётган ҳужумларни албатта инобатга олиш зарур.

3-БОБ. ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАРГА АСОСЛАНГАН КРИПТОБАРДОШЛИ КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИ ВА УЛАРНИНГ ДАСТУРИЙ ТАЪМИНОТИ

3.1. Эллиптик эгри чизиқли алгоритмларни параметрли кўринишга ўтказиш усули

Носимметрик криптографиянинг математик асоси бўлиб бирор алгебраик структура (АС) ва унда криптографик алгоритмга асос қилиб олинган яширин йўлли (махфийликка эга) бир томонлама функция хизмат қилади. АС деганда бирор тўплам ва алгебраик амаллар жуфтлиги тушунилади [9]. Криптографик алгоритмнинг ҳар хил ташқи ва ички ҳужумларга бардошлилиги АС бир томонлама функциясини тескарилаш мураккаблигига асосланади.

1985 йилдан бошлаб Н.Коблиц [10, 11] ва В.Миллер [12] таклиф этган носимметрик криптографиянинг традицияга айланиб қолган криптотизимларидан бардошлилиги ЭЭЧ группасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларга ўтиш бошлангани кўзга ташланди. Эллиптик криптографияга алоҳида қизиқиш қуйидаги сабаблар [13] билан белгиланади:

- биринчидан, дискрет логарифмлаш ва факторлаш муаммоларини ечишга қаратилган сонли майдонларда n модули бўйича сонлар силлиқлиги хоссасидан фойдаланадиган умумлашган ғалвир усулига асосланган тезкор алгоритмларнинг юзага келиши. ЭЭЧ группасида эса силлиқлик тушунчаси аниқланмаганлиги уларда тезкор криптотаҳлиллаш алгоритмларини тузиш имкониятини бермайди, бу ерда силлиқ сон унча катта бўлмаган туб сонлар кўпайтмаси;

- иккинчидан, ЭЭЧ группасида калит узунлиги бўйича криптотизимлар ишлаб чиқариш афзалликларга эга эканлиги. Булар симсиз коммуникацияларда ва ресурс чекланган ҳолларда (смарт-карталар, мобиль қурилмалар) асосий ҳисобланади. Масалан, ЭЭЧ группасида тузилган калитнинг бинар узунлиги *150* дан *350* гача бўлган қурилмаларда анъанавий қурилмалардаги калитнинг бинар узунлиги *600* дан *1400* гача бўлгандагидек криптографик бардошлилик даражасига эришилади.

Юқорида келтирилган сабаблар АҚШ ва Россия Федерациясида амалдаги стандартларни эллиптик криптографияга оид стандартлар билан алмаштиришга олиб келди. Ҳозирги кунда ЭЭЧларга асосланган алгоритмлар кўплаб халқаро, миллий ва соҳага оид стандартлар қаторидан ўрин олган. Эллиптик криптографияда туб майдон *GF(p)*да берилган ЭЭЧдан кенг фойдаланилади. *GF(p)*да берилган ЭЭЧ тенгламаси $y_0^2 \equiv x_0^3+ax_0+b \ (mod\ p)$ кўринишга эга.

Фан-техника ва маркетинг тадқиқотлари маркази («UNICON. UZ».ДУК) нинг «Ахборот хавфсизлиги ва криптология» илмий-тадқиқот департаментида диаматрицалар алгебрасини криптология масалалари учун такомиллаштириш натижасида 1999 йилда диамарицавий устунлар АС ва параметрли АС юзага келди [9]. Натижада аввал маълум бўлган махфийликка қўшимча махфийлик киритиш орқали ҳужумларга бардошлиликни янада ошириш мақсадида ундан янгича фойдаланиш имконияти туғилди. Шундан буён такомиллашган диаматрицавий ва параметрли алгебралар ҳамда параметрли ЭЭЧ группаси ахборотни ҳимоялаш воситаларини ишлаб чиқиш ва криптотаҳлил жараёнларини амалга оширишда математик база сифатида фойдаланилмоқда.

Параметрли АС

Элементлари бир хил *a* ва *b* лардан таркиб топган *m* x *1* тартибли диаматрицавий устунлар *A* ва *B* дан битта элементли *a* ва *b* лардан таркиб топган *1* x *1* тартибли устунларга ўтилса, параметрли кўпайтириш амали қуйидаги кўринишда ифодаланиб

$a \circledR b \equiv a + b + aRb \ (mod\ n)$ (1)

формула асосида аниқланади.

Параметрли тескари элемент қуйидагича ҳисобланади:

$a^{\backslash -1} \equiv -a(1+ aR)^{-1} \ (mod\ n).$ (2)

Бу ерда $^{\backslash -1}$ - *n* модуль бўйича параметрли тескарилаш, $^{-1}$ - *n* модуль бўйича тескарилаш амалининг рамзи.

Оқибатда параметрли АС (*GF(n); ®)* кўринишига эга бўлади; бу ерда *GF(n)* – *n* тартибли бутун сонлар чекли тўплами, ® - *GF(n)* элементлари устида параметрли кўпайтириш амалининг рамзи.

Параметр муаммоси

Параметр муаммоси тўртта мураккаблик поғонаси билан фарқланади:

Агар параметрли АС *(GF(n); ®)* да ташувчи *GF(n)*нинг

- элементи $y \equiv a^{\backslash x} (mod\ n)$ берилган бўлса, унда параметр *R,* даража кўрсаткичи *x* ва элемент *a* топилсин, *(3*-поғона*),*

- элементлар *y* ва *a* берилган бўлса, унда параметр *R* ва даража кўрсаткичи *x* топилсин *(2*-поғона*),*

- элементлар *y* ва даража кўрсаткичи *x* берилган бўлса, унда параметр *R* ва элемент *a* топилсин, *(1*-поғона*),*

- элементлар *y, a* ва даража кўрсаткичи *x* берилган бўлса, унда параметр *R* топилсин, бу ерда $R > a+2^{160}$, *(0*-поғона*).*

Бу ерда *GF(n)– n* та бутун сонлардан тузилган чекли тўплам.

Мазкур муаммонинг юзага чиқиши бир томонлама параметрли функциянинг қуйидаги хоссаси билан боғлиқ:

$a^{\backslash x} \equiv a \Sigma_{i=0}^{i=x-1} F^i\ (mod\ n)$, бу ерда $F=1+Ra.$ (3)

Мазкур муаммо параметрли ЭЭЧ группасида хам ўхшаш талқинга эга. Унда элемент ўрнида нуқтанинг *x-, y-* координаталари жуфтлиги қатнашади.

3.2. Параметрли Диффи-Хеллман калит алмашиш алгоритми

Фараз қилайлик, *j*-томон параметрли алгебра асосида такомиллаштирилган Диффи-Хеллман калит алмашиш алгоритми асосида ишлайдиган тизимга, *i*-томон эса мавжуд Диффи-Хеллман 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

$y_j \equiv (a\text{-}1)^{\backslash dj}+1(mod\ p)$ 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,

$k_j \equiv (y_i\text{-}1)^{\backslash dj} +1(mod\ p)$ 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 $k=k_i= k_j$.

Параметрли Диффи-Хеллман калит алмашиш алгоритмига оид мисол қуйидаги 6-жадвалда келтирилган:

6-жадвал

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.

3.3. Параметрли эллиптик эгри чизиққа асосланган Диффи-Хеллман калит алмашиш алгоритми

Параметрли эллиптик эгри чизиқли Диффи-Хеллман калит алмашиш алгоритми эллиптик эгри чизиқли Диффи-Хеллман алгоритмига нисбатан криптобардошлиги юқори ҳисобланади. Эллиптик эгри чизиқли алгебрадан параметрли алгебрага ўтиш қуйидагича амалга оширилади:

ЭЭЧ тенгламасидан параметрли ЭЭЧ (ПЭЭЧ) тенгламасига ўтиш.

Хосса. Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$ ва $y_0^{\ 2} \equiv x_0^{\ 3}+ax_0+b \pmod p$ лар ўзаро изоморф бўлса, у ҳолда

- $B \equiv (a+b)\, R^{-1} \pmod p$,
- $y \equiv (y_0-1)\, R^{-1} \pmod p \equiv (x^{\backslash 3}+ax+B)^{\backslash 0.5} \pmod p$,
- $y - \equiv -(y_0+1)\, R^{-1} \pmod p \equiv -(y+2R^{-1}) \pmod p$,
- $y^{\backslash 2} \equiv (y_0^{\ 2}-1)\, R^{-1} \pmod p$,
- $x \equiv (x_0-1)\, R^{-1} \pmod p$,
- $x^{\backslash 3} \equiv (x_0^{\ 3}-1)\, R^{-1} \pmod p$.

Параметрли ЭЭЧ нуқтасининг чекли аддитив группа элементига мослиги.

Хосса. Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$ *ПЭЭЧ* таққосламаси бўлиб, $Y=(x,y)=d*^{\backslash}G$ нуқта шу таққосламани қаноатлантирса, у ҳолда *ПЭЭЧ* нуқтаси *x-*, *y-* координаталарига чекли q тартибли аддитив группа $(GF(p);"+")$ нинг элементлари $x= d*g_1 \pmod q$, $y = d* g_2 \pmod q$ ўзаро мос келади, бу ерда "$*^{\backslash}$" - параметрли кўпайтириш, "+" - қўшиш, "*" - кўпайтириш амаллари рамзлари, $G=(g_1, g_2)$.

ПЭЭЧ нуқтасининг чекли q тартибли аддитив группа элементига мослиги хоссасидан фойдаланиш *ЭЭЧ*ларда дискрет логарифмлаш масаласини чекли аддитив группанинг базис элементини топиш асосида ҳал этишга йўл очади.

a, B - бутун сонли коэффициентлар,

R – параметр, $0<R< n, (R; n)=1$ шартларини қаноатлантиради**.**

$Q_1=(x_1, y_1)$ ва $Q_2=(x_2, y_2)$ нуқталар устида ***параметрли қўшиш*** амали "$+^{\backslash}$ **"** билан белгиланади ва $Q_3 = Q_1 + {}^{\backslash}Q_2$ кўринишида ифодаланади. (x_1, y_1) ва (x_2, y_2) нуқталар устида ***параметрли қўшиш*** қуйидаги таққосламалар асосида амалга оширилади:

1) $x_1 \neq x_2$ ҳол учун $Q_3=(x_3, y_3)$**:**

$$x_3 \equiv (L^2-3)R^{-1}-x_1- x_2) \pmod p, \qquad (4)$$

$$y_3 \equiv L(x_1- x_3)+ y_1^{-} \pmod p, \qquad (4')$$

бу ерда:

$$L \equiv (y_2- y_1)\,(x_2- x_1)^{-1} \pmod p;$$

2) $x_1=x_2$, $y_1= y_2 \neq 0$ ҳол учун $Q_3=(x_3, y_3)$**:**

$$x_3 \equiv (L^2-3)R^{-1}-2x_1 \pmod p, \qquad (5)$$

$$y_3 \equiv L(x_1- x_3) + y_1^{-} \pmod p, \qquad (5')$$

бу ерда: $L \equiv (3(R\,x_1^{\backslash 2}+1)+a)(2(R\,y_1+1))^{-1} \pmod p$;

3) $x_1=x_2$, $y_2=-y_1$ ҳол учун $Q_1=(x_1, x_2)$ ва $Q_2=(x_2, -y_1)$ нуқталарнинг ***параметрли*** йиғиндиси ноллик (чексизликдаги) нуқта 0_E га тенг.

Ноллик нуқта учун $Q+^{\backslash} 0_E = 0_E +^{\backslash} Q = Q$ (6)

тенглик ўринлидир.

ЭЭЧ нуқтасини ўзига ўзини d марта параметрли қўшиш натижаси нуқтани скаляр сон d га кўпайтириш амалини беради. ЭЭЧ нуқтасини скаляр сон d га кўпайтириш амали " $*^{\backslash}$ " белгиси билан ифодаланади.

Шуни таъкидлаш керакки, Вейерштрасс [56-58] умумий кўринишдаги тенгламасининг қолган барча хусусий ҳоллари бўлган ЭЭЧ тенгламалари учун ҳам юқорида келтирилган ЭЭЧ нуқталари устида параметрли қўшиш $+^{\backslash}$ ва ЭЭЧ нуқтасини скаляр сон d га кўпайтириш амали $*^{\backslash}$ ни аниқлаш ҳеч қандай қийинчилик туғдирмайди.

ЭЭЧ барча нуқталари устида параметр $R \geq 1$ билан қўшиш амали чекли аддитив коммутатив группани ташкил этади.

Таъриф. $PE(F_n) = \{$параметрли ЭЭЧ нуқталари$\} \cup \{0_E\}$, яъни параметрли ЭЭЧ барча нуқталари тўплами ва ноллик нуқта, параметр $0<R\in F_n$ бўлса, $+^{\backslash}$ – $PE(F_n)$ устида аниқланган параметрли қўшиш амали бўлса, $(PE(F_n);\ +^{\backslash})$ – жуфтлик параметрли ЭЭЧ нуқталари группаси деб аталади.

Анъанавий ЭЭЧ ва параметрли ЭЭЧ нуқталари тўпламлари ўзаро изоморфлиги туфайли ***аддитив коммутатив группанинг*** барча аксиомалари параметрли ЭЭЧ нуқталари группасини ҳам қаноатлантиради.

Бу ҳолат параметрли ЭЭЧ нуқталари группаси асосида қўшимча махфийликка эга бўлган бир томонлама функциялар асосида мавжуд криптотизимларга аналог бўлган янги криптотизимларни ва янги криптотаҳлиллаш усулларини яратишга йўл очади.

Аввалги бандда келтирилган параметрли ЭЭЧ нуқталари группаси $(PE(F_p);\ +^{\backslash})$ дан фойдаланиш қўшимча махфий параметр R туфайли ҳозирча маълум бўлмаган ошкормас ЭЭЧ параметри муаммоси юзага келиши ва бунинг оқибатида криптобардошлилик ортиши қайд этилган эди.

Параметрли ЭЭЧлардан фойдаланишга асосланган алгоритмлар бардошлилиги улар махсус аппаратли модуль сифатида амалга оширилганда энг юқори даражада бўлиши [55] да изоҳланган.

Таъриф. $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \ (mod\ p)$ таққосламани қаноатлантирувчи ЭЭЧ нуқталари группаси $PE(F_p)$ да ЭЭЧ нуқтасини параметрлар учлиги $<R, a, B>$ билан скаляр сонга кўпайтириш ($*^{\backslash}$) функцияси параметрли ЭЭЧ функцияси деб аталади.

Бу ерда:

$y \equiv (x^{\backslash 3}+ax+B)^{\backslash 0.5} (mod\ p)$,

$y^{-} \equiv -(y+2R^{-1})\ (mod\ p)$,

a, B – бутун сонли коэффициентлар,

R – параметр, $0 < R < p, (R; p)=1$ шартларини қаноатлантиради**,**

q – параметрли ЭЭЧ нуқталари тартиби,

p – туб сон.

G нуқтани скаляр сон d га параметрли кўпайтириш натижаси $d*^{\backslash}G$ шаклида ифодаланган, $^{\backslash}$ – R параметрли даражага ошириш белгиси, $*^{\backslash}$ – скаляр сонга параметр R билан кўпайтириш белгиси**.**

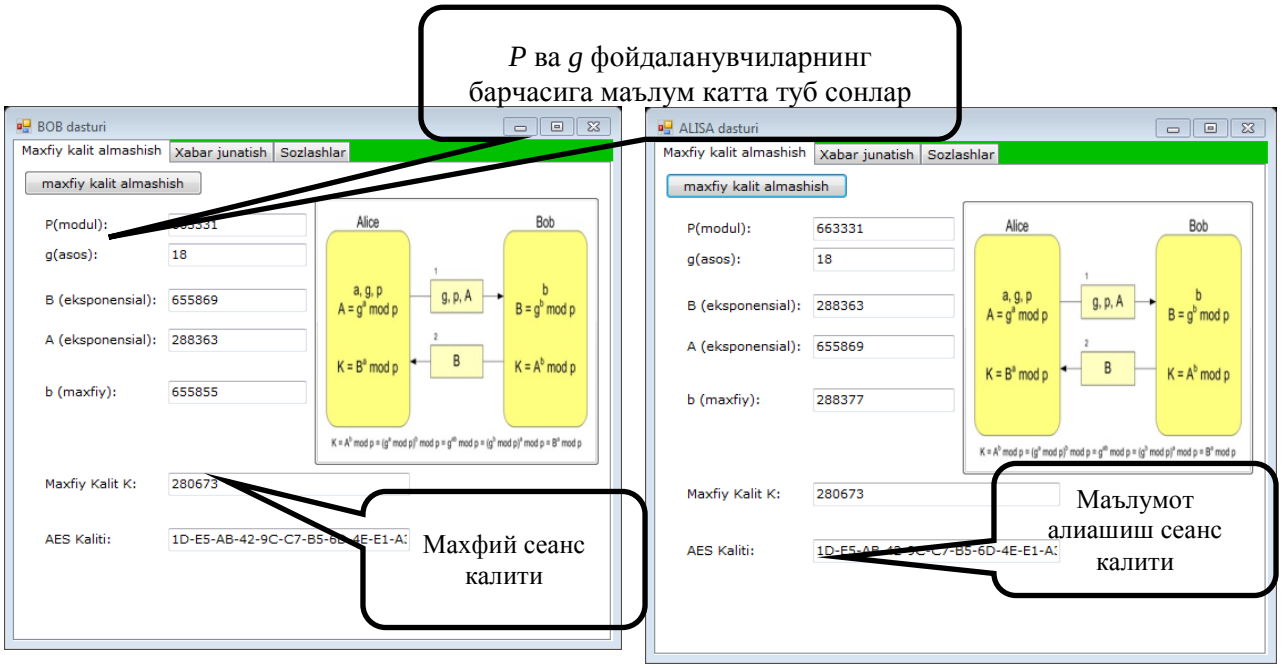
Параметрли ЭЭЧ функцияси хоссалари анъанавий ЭЭЧ функцияси хоссаларига ўхшаш бўлиб, параметрли ЭЭЧ функцияси қийматини исталган скаляр сон учун самарали ҳисоблаш учун етарлидир. Бу ерда, катта скаляр сонга параметрли кўпайтириш жараёни экспоненциал функцияни ҳисоблаш жараёни каби кечиб, d ни 2 нинг даражалари йиғиндиси сифатида ифодалашга ва даврий тарзда йиғиндини ташкил этувчи 2 нинг даража кўрсаткичи, агар жуфт қийматли бўлса, 2 га параметрли кўпайтириш, акс ҳолда жорий қийматни берилган нуқтага параметрли кўпайтириш амалларидан фойдаланишдан иборат бўлади. Бу хоссалар анъанавий ЭЭЧ функцияси хоссаларидан фойдаланишга асосланган криптографик тизимларга ўхшаш криптотизимлар яратишга имкон беради.

3.4. Диффи-Хеллман калитларни тақсимлаш алгоритми асосида дастурий таъминот ишлаб чиқиш

Дастурий таъминотнинг ташқи кўриниши.

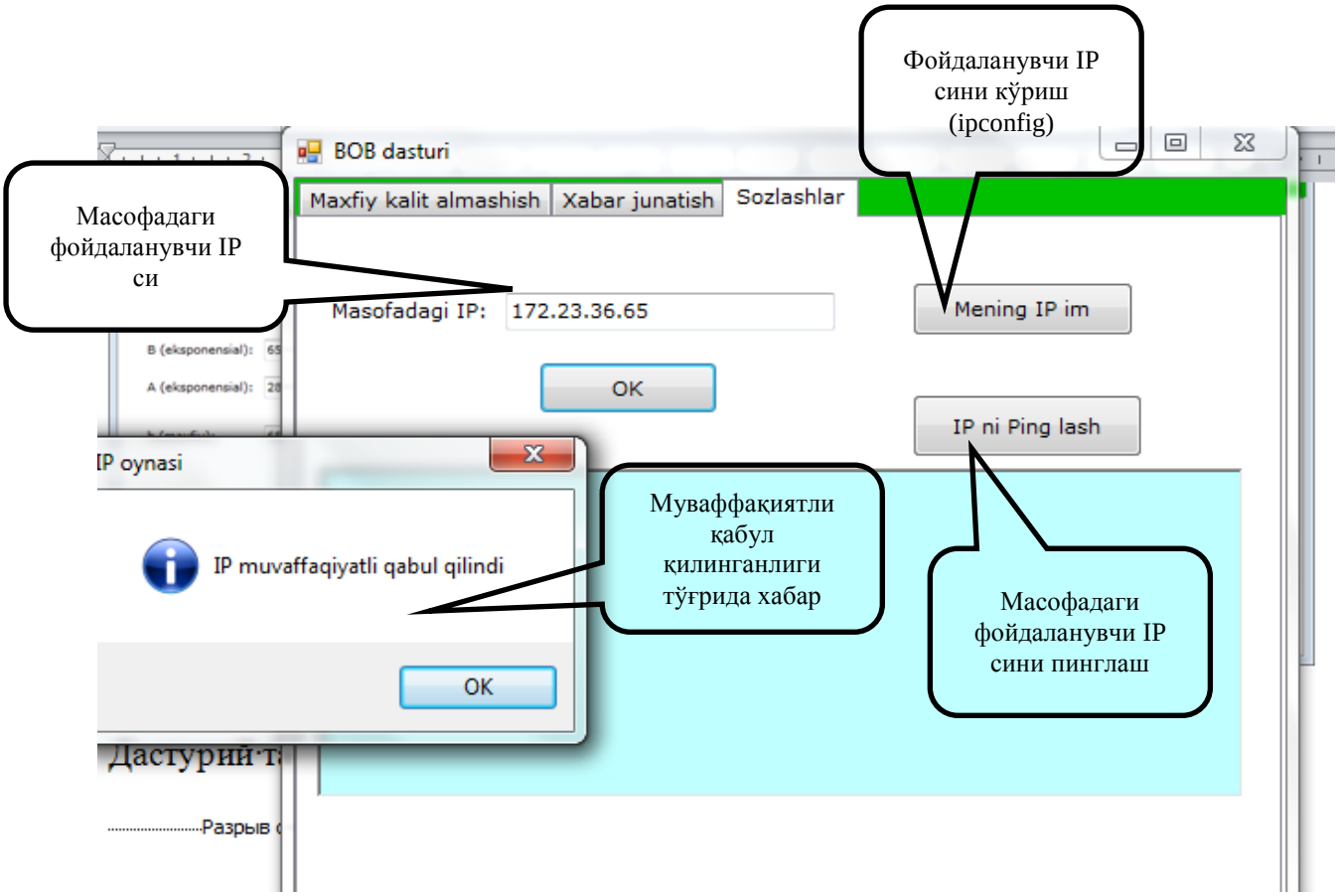
Дастурий таъминотда калит алмашиниш жараёни Диффи-Хеллман алгоритми асосида амалга оширилади. Бу калит алмашиш жараёнини ҳимояланмаган телекоммуникациялар тармоғида амалга ошириш имкониятини туғдиради. Калитлар алмашиш жараёни бажарилгандан сўнг

икки тараф ҳам бир-биридан мустақил равишда ўзининг сеанс калитига эга бўлади. Шу умумий сеанс калити орқали иккала томон ҳам мустақил равишда AES (Advanced Encryption Standart) калитини генерация қилади. Бу асосида ҳар иккала тараф ҳимояланган тарзда маълумот алмашиш ҳуқуқига эга бўлади. Бу қуйидаги 20-расмда келтирилган:



Дастурий таъминотнинг созлаш ойнаси.

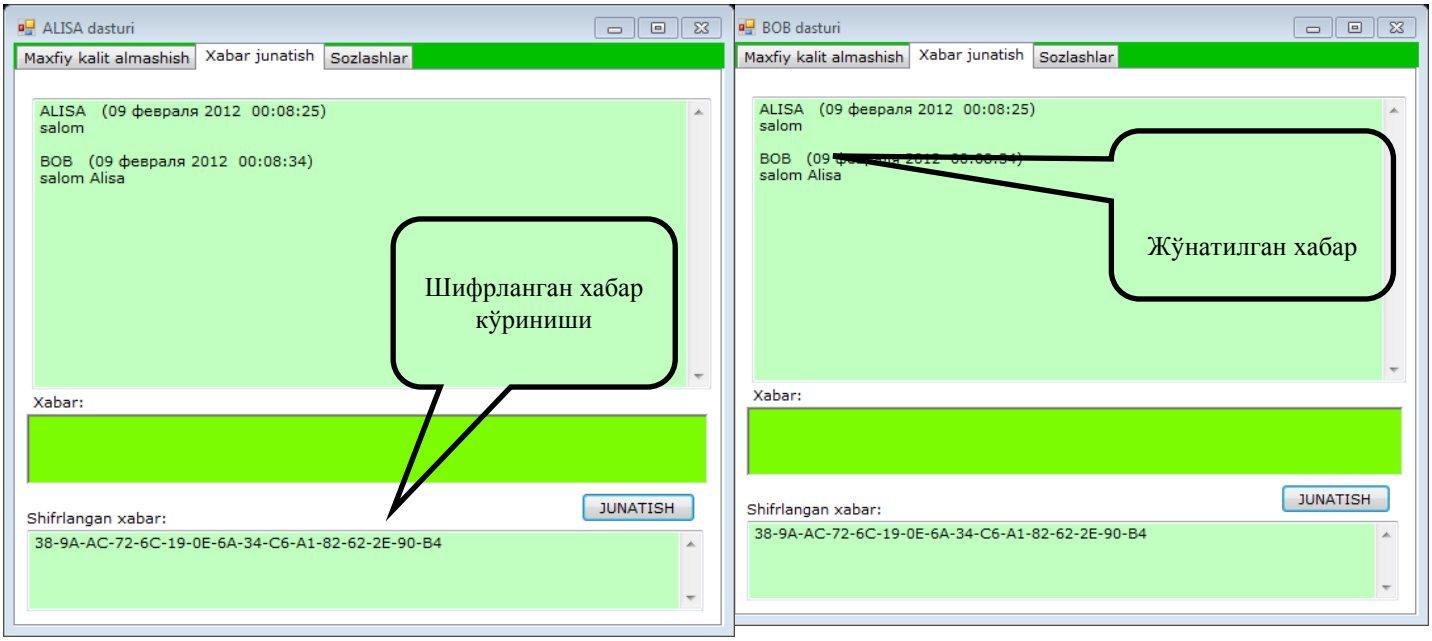
Дастурий таъминотнинг созлаш ойнасида масофадаги(тармоқдаги) фойдаланувчи IP си киритилади. Бундан ташқари ўзининг IP сини аниқлаш ҳамда масофадаги фойдаланувчини **ping** лаш имконияти ҳам мавжуд. Бу қуйидаги 21-расмда келтирилган.



21-расм. Дастурий таъминотнинг созлаш ойнаси

Дастурий таъминотнинг маълумот алмашиш жараёни.

Бу хабар жўнатиш бўлимида иккала фойдаланувчи хавфсиз тарзда маълумот алмашиш жараёнини амалга ошириши мумкин (22-расм).

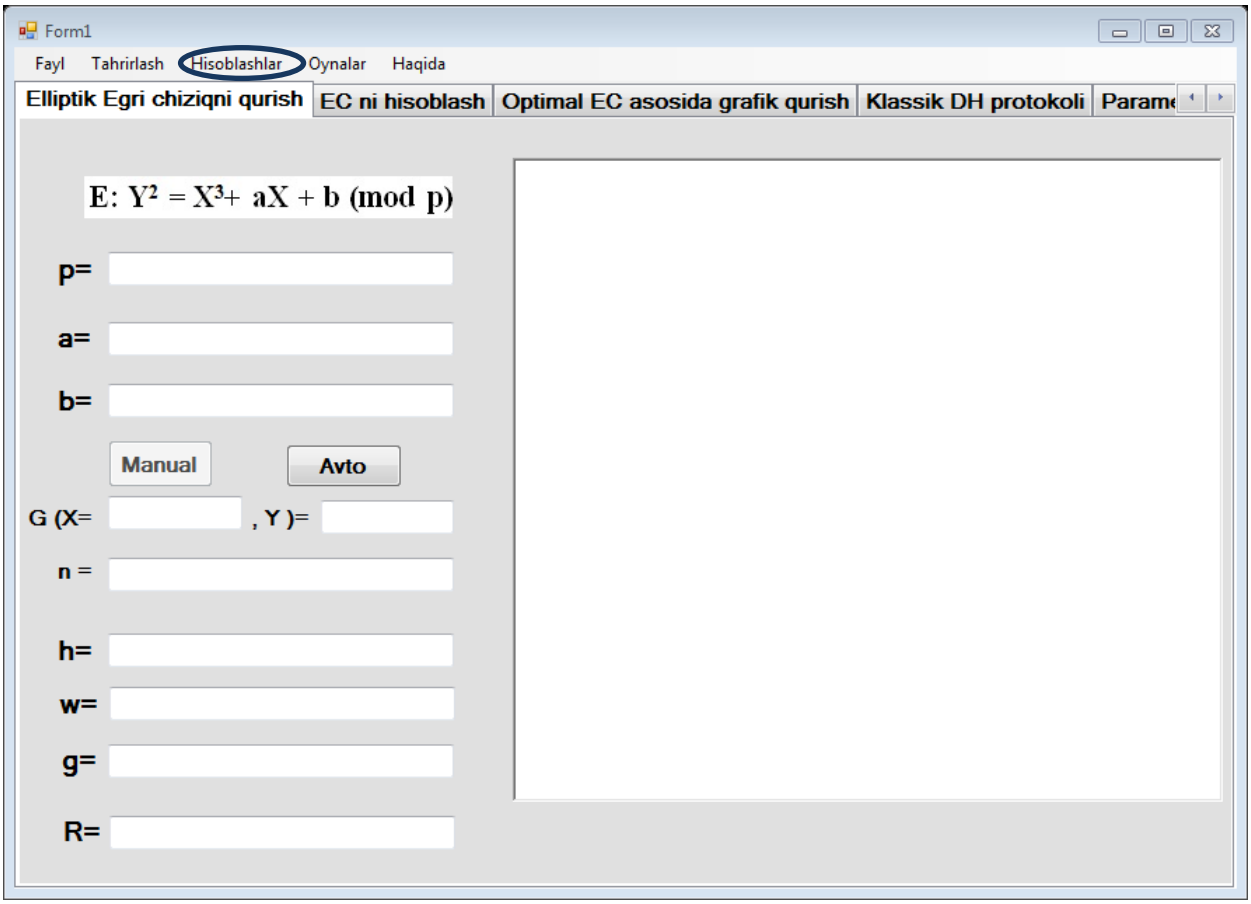


22-расм. Дастурий таъминотнинг маълумот алмашиш жараёни

3.5. Эллиптик эгри чизиқли ва параметрли Диффи-Хеллман алгоритмлари асосида дастурий таъминотларни яратиш

Дастур ойнасининг умумий кўриниши:

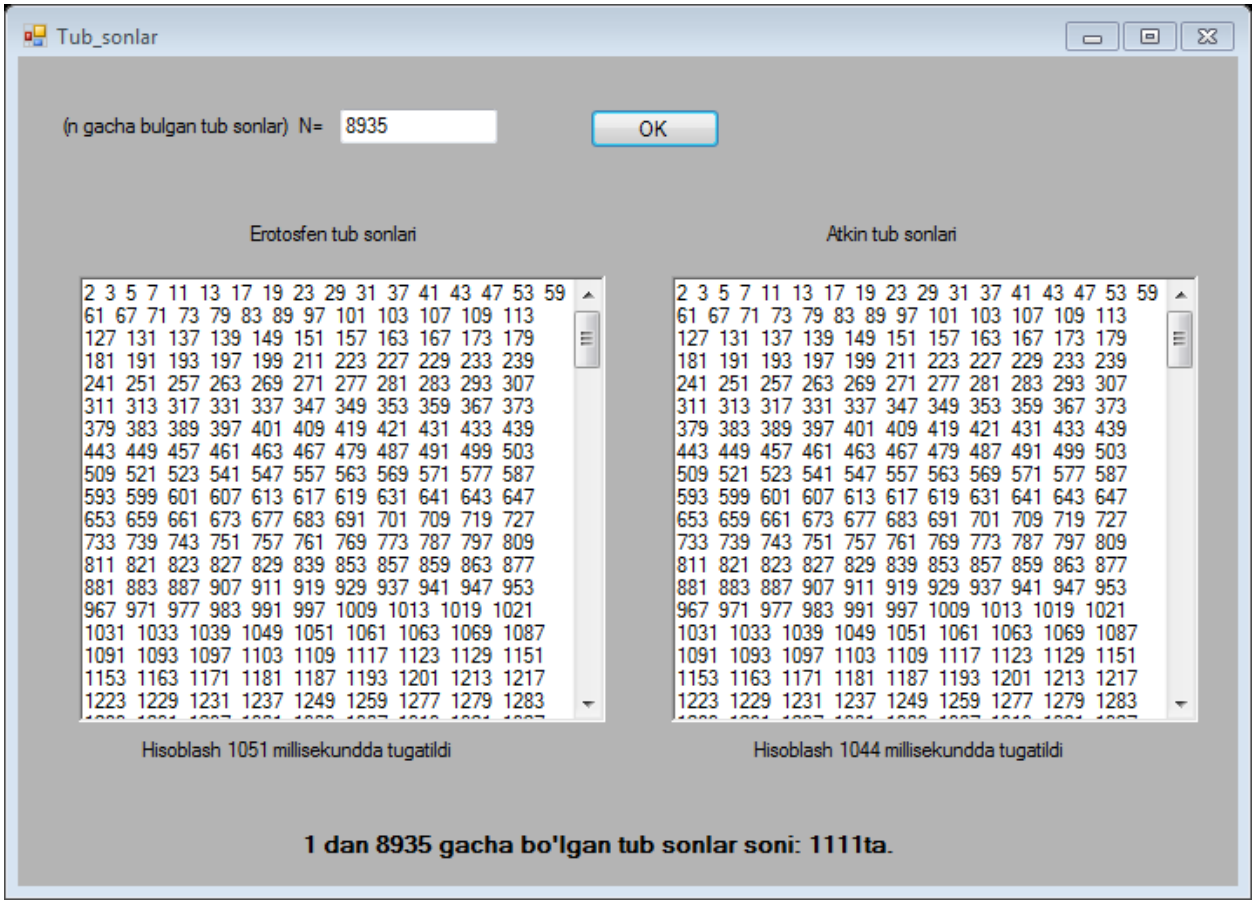
Эллиптик эгри чизиқни қуриш ва умумий параметрларни танлаш бажарилади. Бунинг учун биринчи навбатда *Hisoblashlar* менюсидан *tub sonlar ro'yxati* ни танлаш ва шу ердан туб сонлар рўйхатини ҳосил қилиш талаб этилади (23-расм).



23-расм. Эллиптик эгри чизиқни ҳисоблаш ойнаси

24-расмда туб сонлар рўйхатини ҳосил қилиш методлари ва уларни тезкорлиги бўйича таҳлили кўрсатиб ўтилган. Бу ерда туб сонлар рўйхатини ҳосил қилиш учун классик ҳисобланган Эротосфен ғалвири ҳамда замонавий ҳамда тезкор ҳисобланган Аткин ғалвири келтириб ўтилган. Эротосфен ғалвири классик асосда туб сонларни берилган рўйхатдан қисқартириш орқали саралаш йўли билан ишлайди. Аткин ғалвири эса квадрат илдиз усули асосида туб сонларни саралайди. Аткин ғалвири Эротосфен ғалвирига

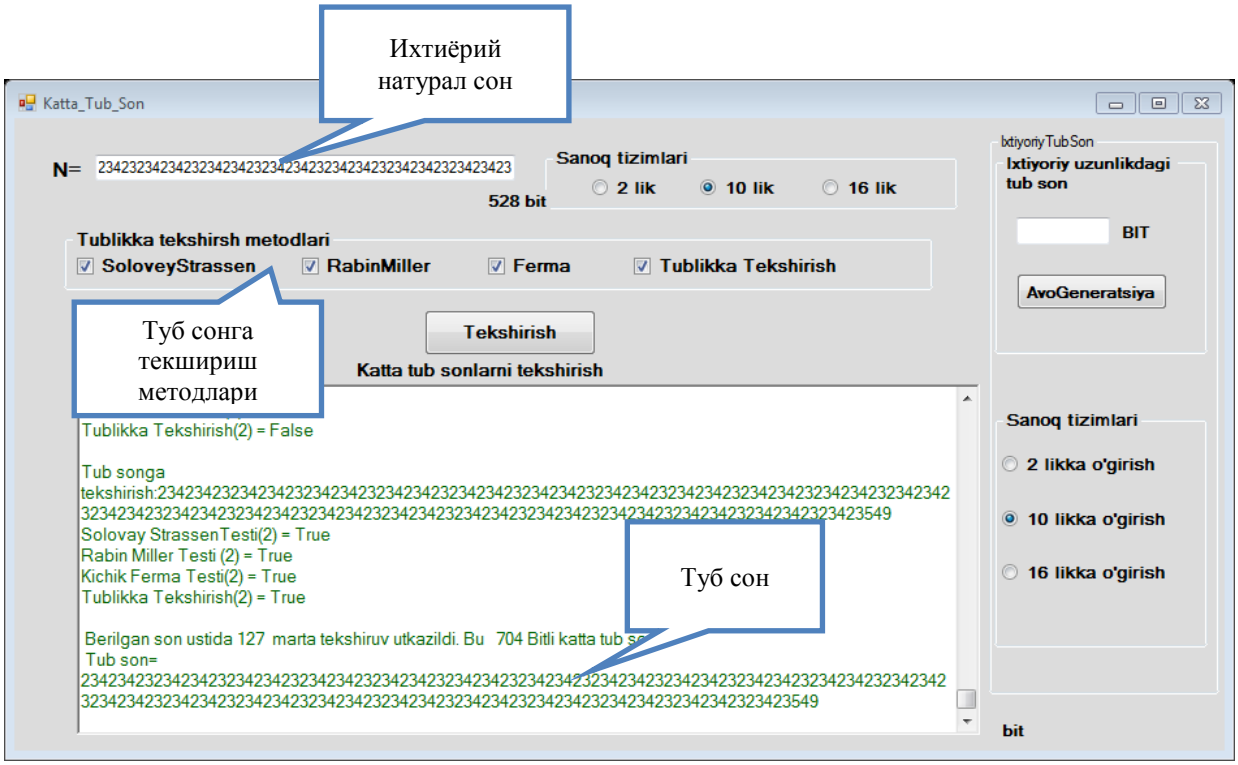
нисбатан тез вақтда берилган сонгача бўлган туб сонлар рўйхатини ҳосил қилади ва у Эротосфен ғалвирига нисбатан замонавийроқ ҳисобланади. Қуйидаги ойнада уларнинг тезлиги бўйича таҳлилни кўришимиз мумкин. Бундан ташқари *1* дан *N* гача бўлган ораликдаги туб сонлар сонини ҳам кўришимиз мумкин. Расмдан кўриниб турибдики Аткин ғалвири Эротосфен ғалвирига нисбатан тезроқ туб сонлар рўйхатини ҳосил қилар экан. Демак, туб сонлар рўйхатини ҳосл қилиш талаб этилса, Аткин ғалвири тезкорлик ва аниқлик бўйича Эротосфен ғалвирига нисбатан яхшироқ кўрсаткичга эга экан.



24-расм. Туб сонлар рўйхатини ҳосил қилиш ва қиёслаш ойнаси

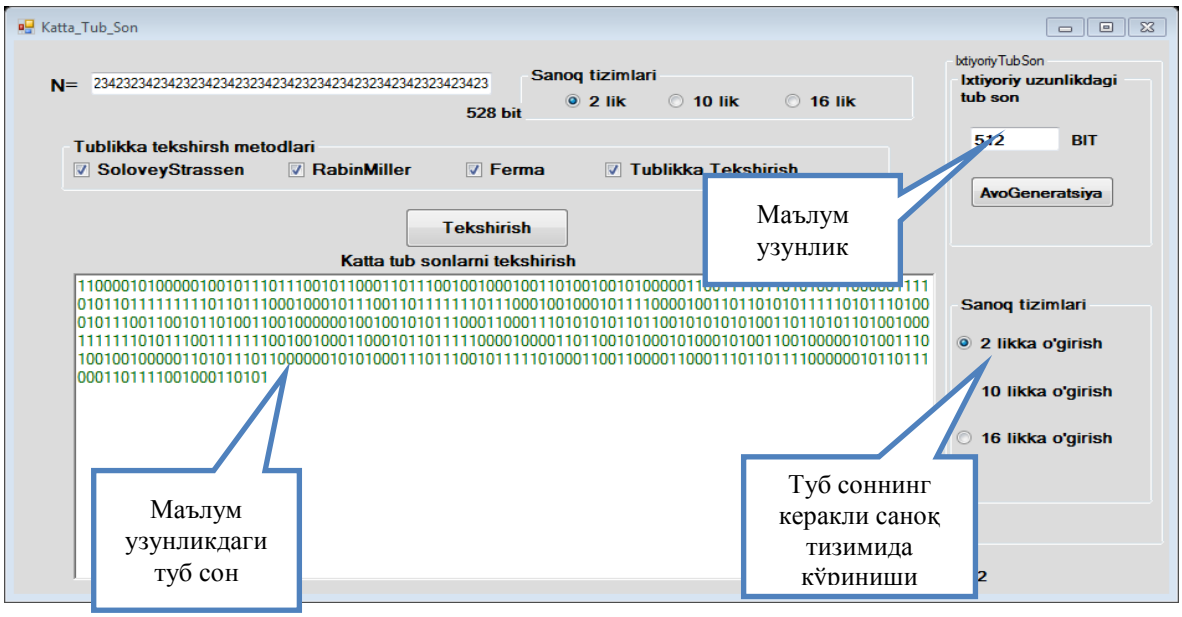
25-расмда жуда катта туб сонларни ҳисоблаш ва ҳосил қилиш методлари тасвирланган. Бу ерда катта туб сонларни ҳосил қилиш методларининг *Соловей Штрассен*, *Рабин Миллер*, *кичик Ферма* ва *маълум узунликдаги туб сонларни текшириш* эҳтимоллик даражаси жуда юқори бўлган жуда катта туб сонларга текшириш мумкин. Саноқ тизимлари иккилик, ўнлик ва ўн олтилик тизимларда ҳар қандай узунликдаги туб сонларни берилган методларда аниқлашимиз мумкин. Жуда катта аниқ туб

сонларни ҳосил қилиш масаласи мураккаб бўлганлиги сабабли, туб сонларни ҳосил қилишда катта сонларни ҳар хил методларда текшириб кўриш талаб этилади ва шу орқали маълум бир узунликдаги катта туб сон олинади. Яъни биз қанчалик кўп методлар асосида сонларни тубликка текширсак, биз шунчалик катта эҳтимоллик билан туб сонларни ҳосил қилишимиз мумкин. Бу дастур ойнасида биз берилган узунликдаги катта натурал сон киритамиз ва текшириш методларини танлаймиз. Биз қанчалик кўп методларни танласак шу даражада эҳтимоллиги катта ва аниқ туб сонни аниқлаб беради, яъни биз киритган сондан кейинги *i*-қадамдаги туб сонни, натурал сондан кейинги келган қайсидир қадамдаги биринчи туб сонни аниқлаб беради. Бу бизга тўлиқ даражада тасодифий туб сонни беради. Яъни бошланғич натурал сон инсон фактори орқали киритиляпти ва шу асосида дастур шу натурал сондан кейинги биринчи туб сонни топиб бизга кўрсатяпти.



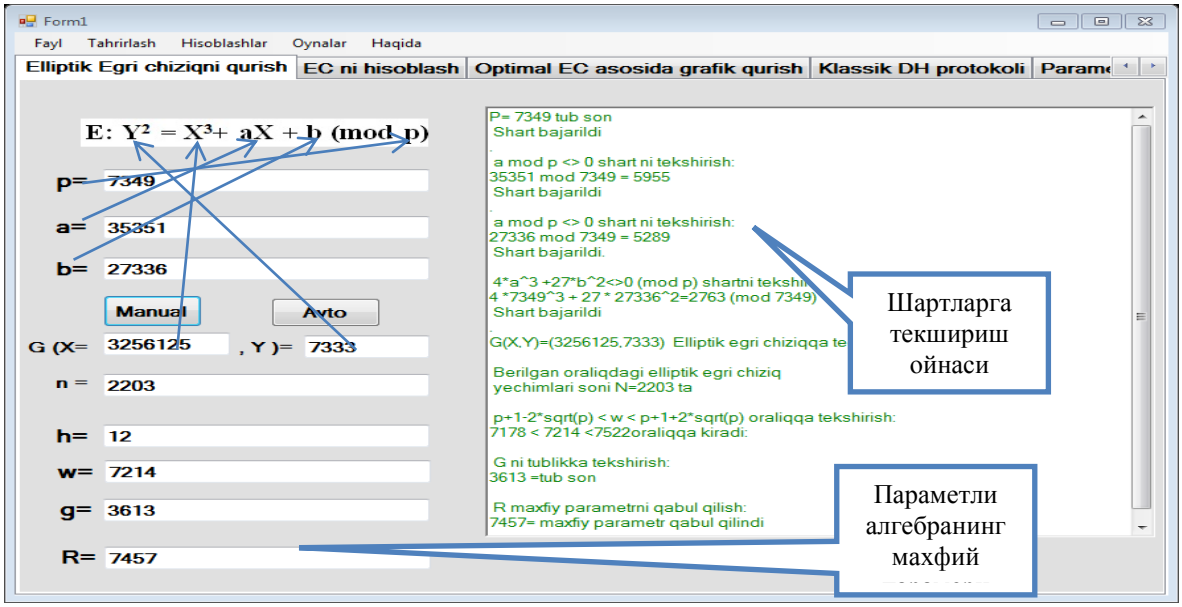
25-расм. Методлар асосида жуда катта туб сонларни тасодифий равишда тубликка текшириш ойнаси

Бундан ташқари керакли узунликдаги псевдотасодифий туб сонларни ҳам ҳосил қилиш мумкинлиги ва уларни иккилик, ўнлик ва ўн олтилик саноқ тизимларига ўтказиб катта узунликдаги туб сонларни талаб қилинган дастурлар учун фойдаланиш мумкинлиги 26-расмда кўрсатилган.



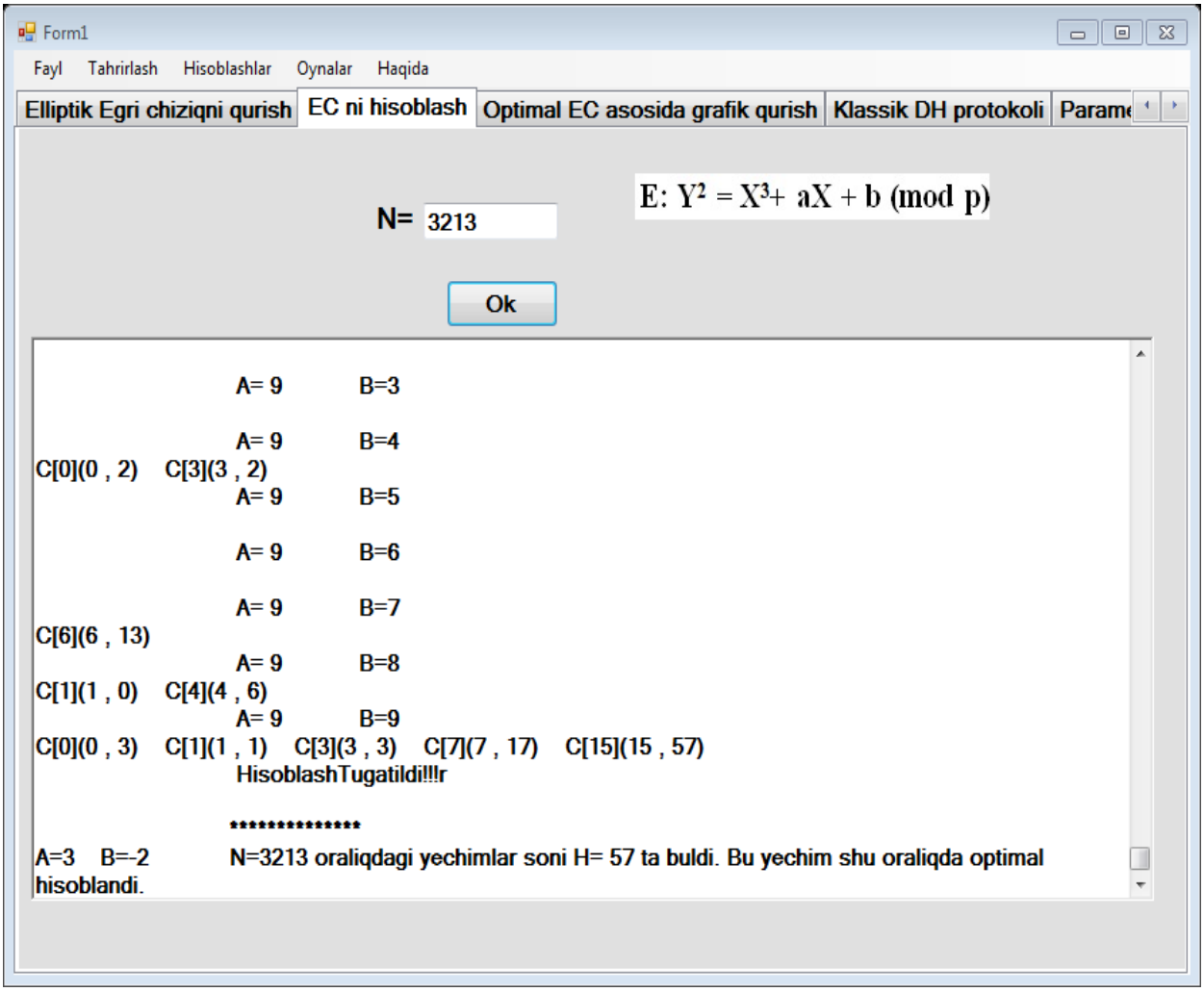
26-расм. Методлар асосида жуда катта туб сонларни псевдотасодифий равишда тубликка текшириш ойнаси

Эллиптик эгри чизиқли, классик ва параметрли *Диффи-Хеллман* алгоритмларини ҳосил қилиш учун умумий параметрларни керакли шарт ва қоидаларга асосланиб танлаб олиниши 27-расмда келтирилган. Бу ойнада автоматик тарзда берилган ораликда керакли параметрларни текшириб қабул қилиб олиши ҳамда киритилган бошланғич параметрларга асосланиб қолган параметрларни генерациялаш имкониятлари мавжуд.



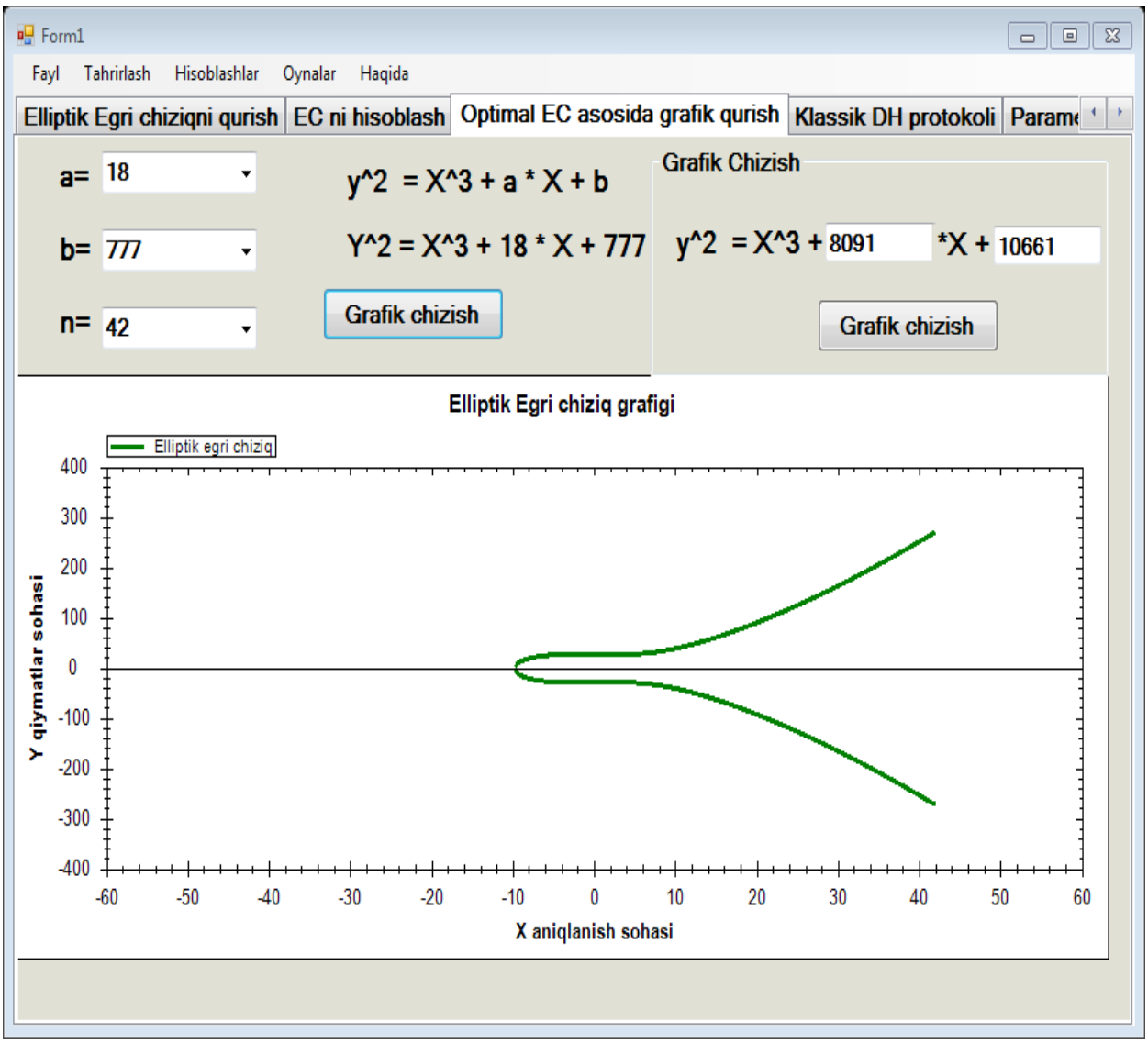
27-расм. Параметрли ва эллиптик эгри чизиқ учун умумий параметрларни ҳосил қилиш

Берилган чекли майдон (n) даги ечимлар сони энг кўп бўлган эллиптик эгри чизиқни танлаб бериш имконини мавжудлиги 28-расмда келтирилган.



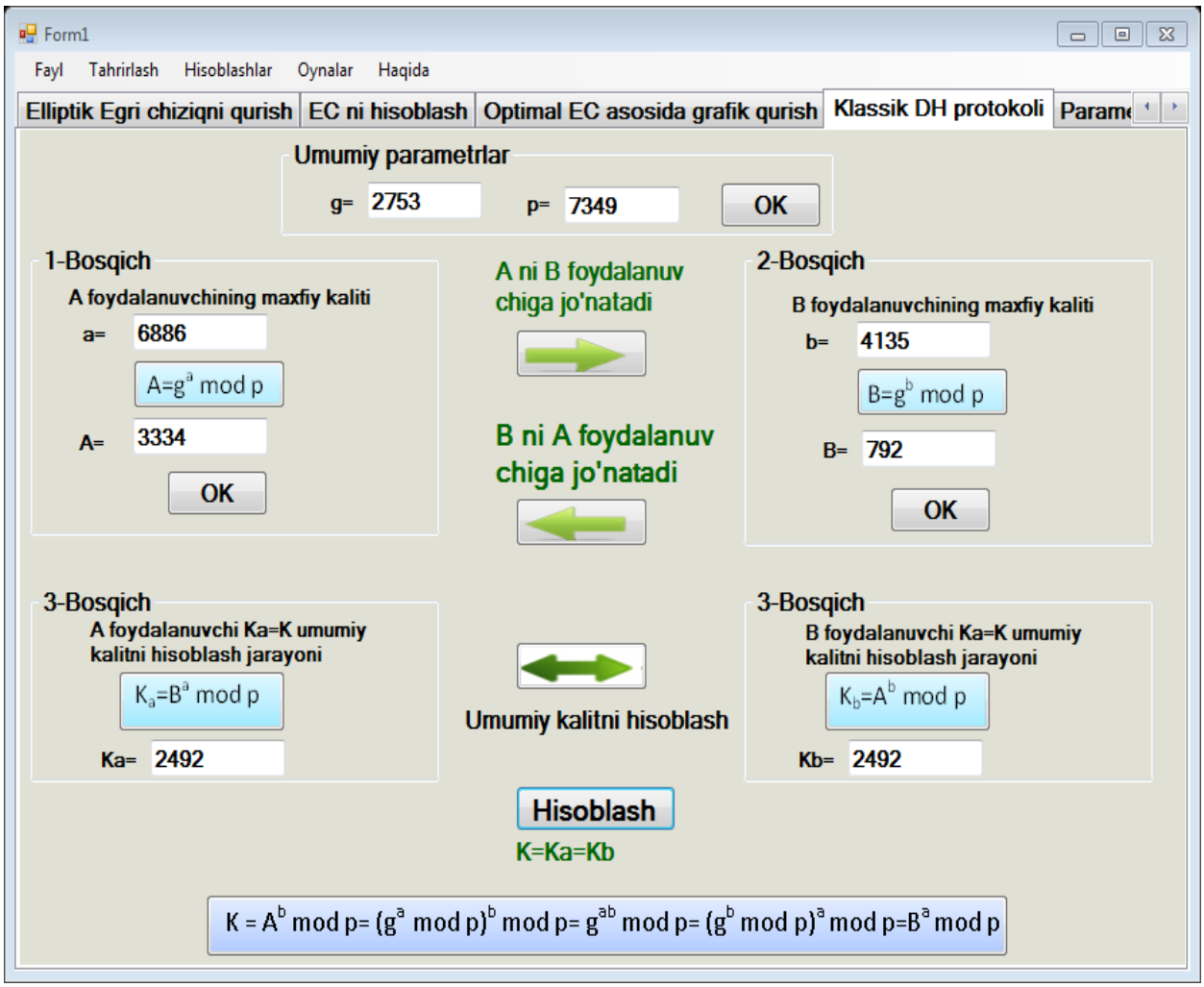
28-расм. Берилган чекли майдонда оптимал эллиптик эгри чизиқни аниқлаш

Қуйидаги 29-расмда биз керакли қийматлардаги эллиптик эгри чизиқ графини қуришимиз ва қандай кўринишда ҳосил бўлишини кўришимиз мумкинлиги келтирилган. Эллиптик эгри чизиқ учун керак бўладиган *a, b* ва *n* параметрлар танлади ва *grafik qurish* тугмаси босилади. Шундан сўнг маълум биз киритган ораликдаги эллиптик эгри чизиқ графигини ҳосил қилишимиз ва шу асосида эллиптик эгри чизиқли криптография учун фойдаланишимиз мумкин.



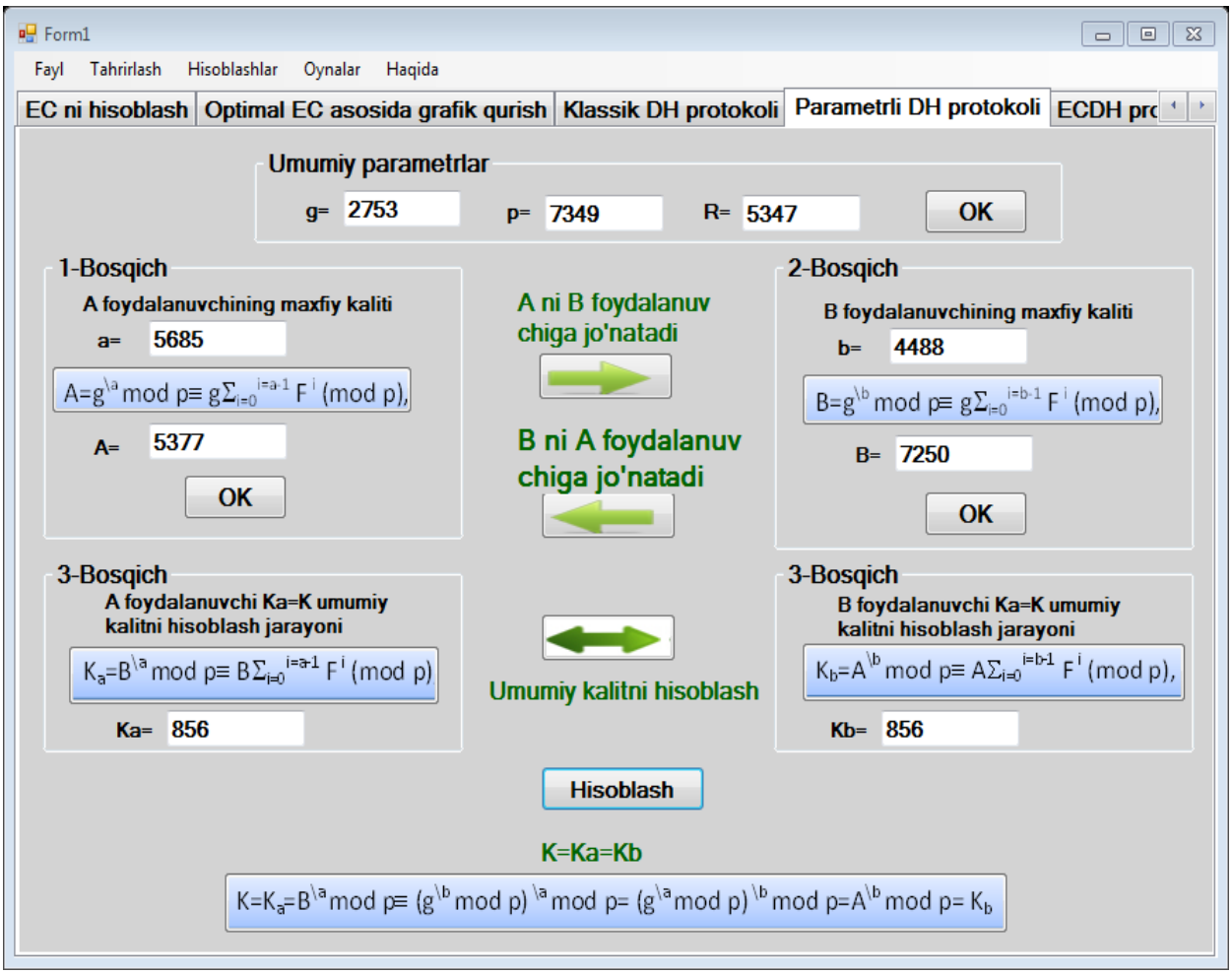
29-расм. Эллиптик эгри чизиқ графигини қуриш

30-расмда классик Диффи-Хеллман алгоритмининг ишлаш структураси босқичма-босқич равишда тасвирланган ва ҳар босқичдаги ҳисоблаш жараёнлари кўрсатиб ўтилган. Биринчи бўлиб олдиндан ҳисоблаб чиқилган умумий параметрлар қабул қилинади. Ундан кейин кетма-кет тарзда классик Диффи-Хеллман алгоритмининг иккита фойдаланувчи ўртасидаги калитларни келишув жараёни тасвирланган. Бу алгоритм дискрет логарифмлаш муаммосига асосланган. Классик Диффи-Хеллман алгоритми бошқа калитларни тақсимлаш алгоритмларига нисбатан жуда яхши криптобардошликка эга ҳисобланади ва тезкорлиги жиҳатидан ҳам анча юқори даражадаги устунликка эгадир.



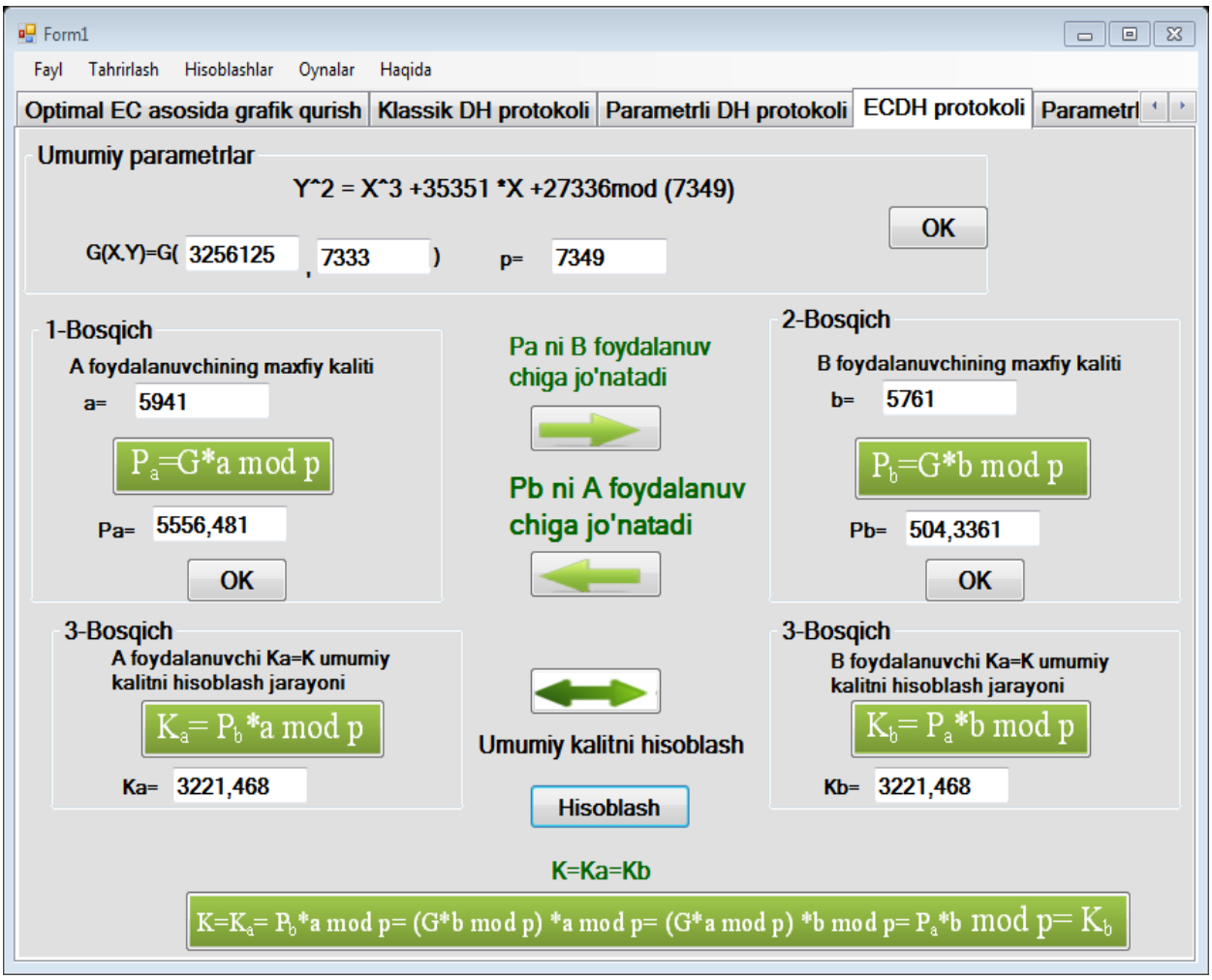
30-расм. Классик Диффи- Хеллман протоколи

31-расмда бу алгоритмнинг криптобардошлигини ошириш мақсадида дискрет логарифлаш муаммосини параметрлар муаммосига алмаштиришимиз мумкинлиги кўрсатилган. Бунда классик даражага кўтариш ўрнига параметрли даражага кўтариш масаласидан фойдаланилади. Бу ерда R қўшимча махфий параметр алгоритм криптобардошлигини оширишига сабаб бўлади, яъни классик $A=g^a(mod\ p)$ ўрнига параметрли алгебрага асосланган даражага кўтариш $A=g^{\backslash a} \equiv a\Sigma_{i=0}^{i=a-1} F^i\ (mod\ p)$, бу ерда $F=1+Rg$ формуласига алмаштирилади.



31-расм. Параметрли Диффи-Хеллман протоколи

32-расмда эллиптик эгри чизиқларга асосланган Диффи-Хеллман алгоритмининг реализацияси тасвирланган. Диффи-Хеллман алгоритмининг муаммоси дискрет логарифмлаш муаммосига асосланганлиги сабабли бу алгоритмни эллиптик эгри чизиқли муаммога ўтказилганда криптобардошлиги ошади ва шунинг ҳисобига калит узунлигининг доимий равишда “инфляция”га учрашини қисқартириш мумкин. Яъни бир хил криптобардошликда кичик узунликдаги калитлардан ҳам фойдаланиш имконини туғдиради. Эллиптик эгри чизиқ тенгламаси асосида янги $G(x,y)$ $y_0^2 \equiv x_0^3+ax_0+b \ (mod \ p)$ ҳосил қилинади. Бу Вейерштрасс тенгламаси ҳисобланади. $G(x,y)$ умумий параметр ҳисобланиб ҳаммага маълум қилинади.



32-расм. Параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман протоколи

Диффи-Хеллман алгоритмининг криптобардошлигини ошириш мақсадида 33-расмда эллиптик эгри чизиқли Диффи-Хеллман алгоритмини параметрли алгебрага асосланган эллиптик эгри чизиқли Диффи-Хеллман алгоритмига ўтказиш келтирилган. Бу ерда қуйидаги амаллар кетма-кетлиги бажарилади.

Эллиптик эгри чизиқ тенгламасидан параметрли эллиптик эгри чизиқ (ПЭЭЧ) тенгламасига ўтиш.

Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \ (mod\ p)$ ва $y_0^{\ 2} \equiv x_0^{\ 3}+ax_0+b \ (mod\ p)$ лар ўзаро изоморф бўлса, у ҳолда

- $B \equiv (a+b)\ R^{-1} (mod\ p)$,
- $y \equiv (y_0-1)\ R^{-1}\ (mod\ p) \equiv (\ x^{\backslash 3}+ax+B)^{\backslash 0.5} (mod\ p)$,
- $y - \equiv -(y_0+1)\ R^{-1}\ (mod\ p) \equiv -\ (y+2R^{-1})\ (mod\ p)$,
- $y^{\backslash 2} \equiv (y_0^{\ 2}-1)\ R^{-1} (mod\ p)$,

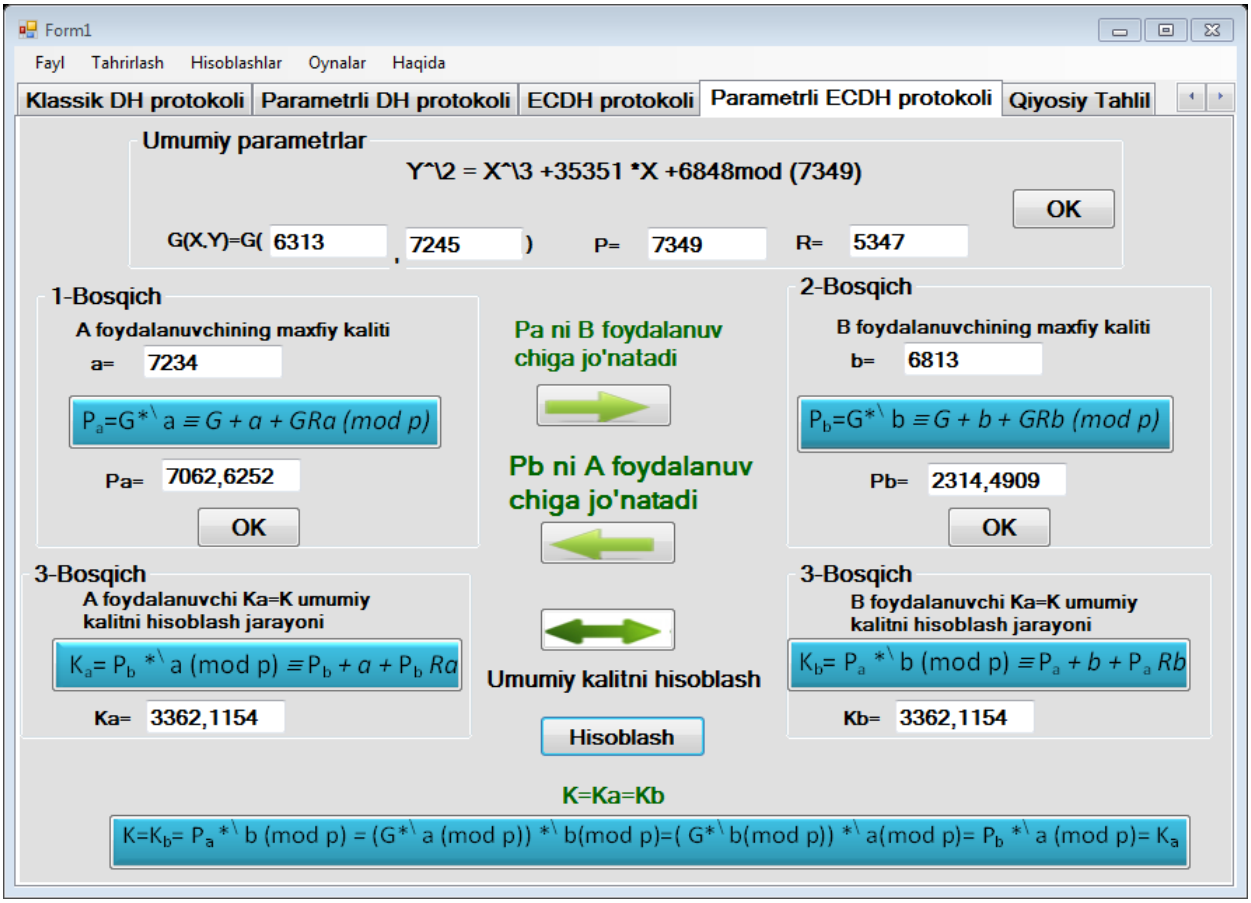
• $x \equiv (x_0\text{-}1)\ R^{-1}\ (mod\ p)$,

• $x^{\backslash 3} \equiv (x_0^{3}\text{-}1)\ R^{-1} (mod\ p)$.

Параметрли ЭЭЧ нуқтасининг чекли аддитив группа элементига мослиги.

Хосса. Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B\ (mod\ p)$ *ПЭЭЧ* таққосламаси бўлиб, $Y=(x,y)=d*^{\backslash}G$ нуқта шу таққосламани қаноатлантирса, у ҳолда *ПЭЭЧ* нуқтаси *x*-, *y*- координаталарига чекли *q* тартибли аддитив группа *(GF(p);"+")* нинг элементлари $x= d*g_1\ (mod\ q)$, $y = d* g_2\ (mod\ q)$ ўзаро мос келади, бу ерда "$*^{\backslash}$" - параметрли кўпайтириш, "+" - қўшиш, "*" - кўпайтириш амаллари рамзлари, $G=(g_1, g_2)$.

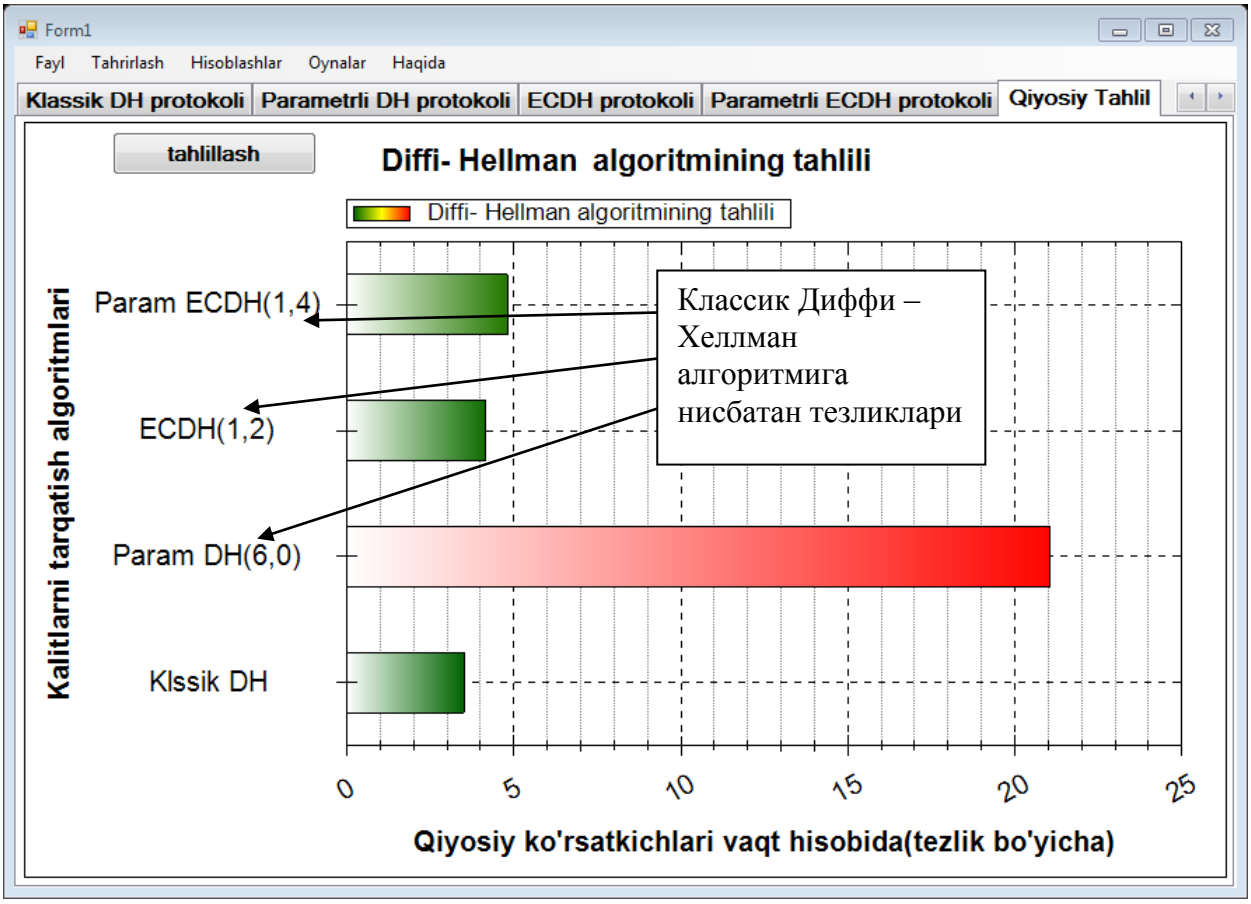
ПЭЭЧ нуқтасининг чекли *q* тартибли аддитив группа элементига мослиги хоссасидан фойдаланиш *ЭЭЧ*ларда дискрет логарифмлаш масаласини чекли аддитив группанинг базис элементини топиш асосида ҳал этишга йўл очади.



33-расм. Параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман протоколи

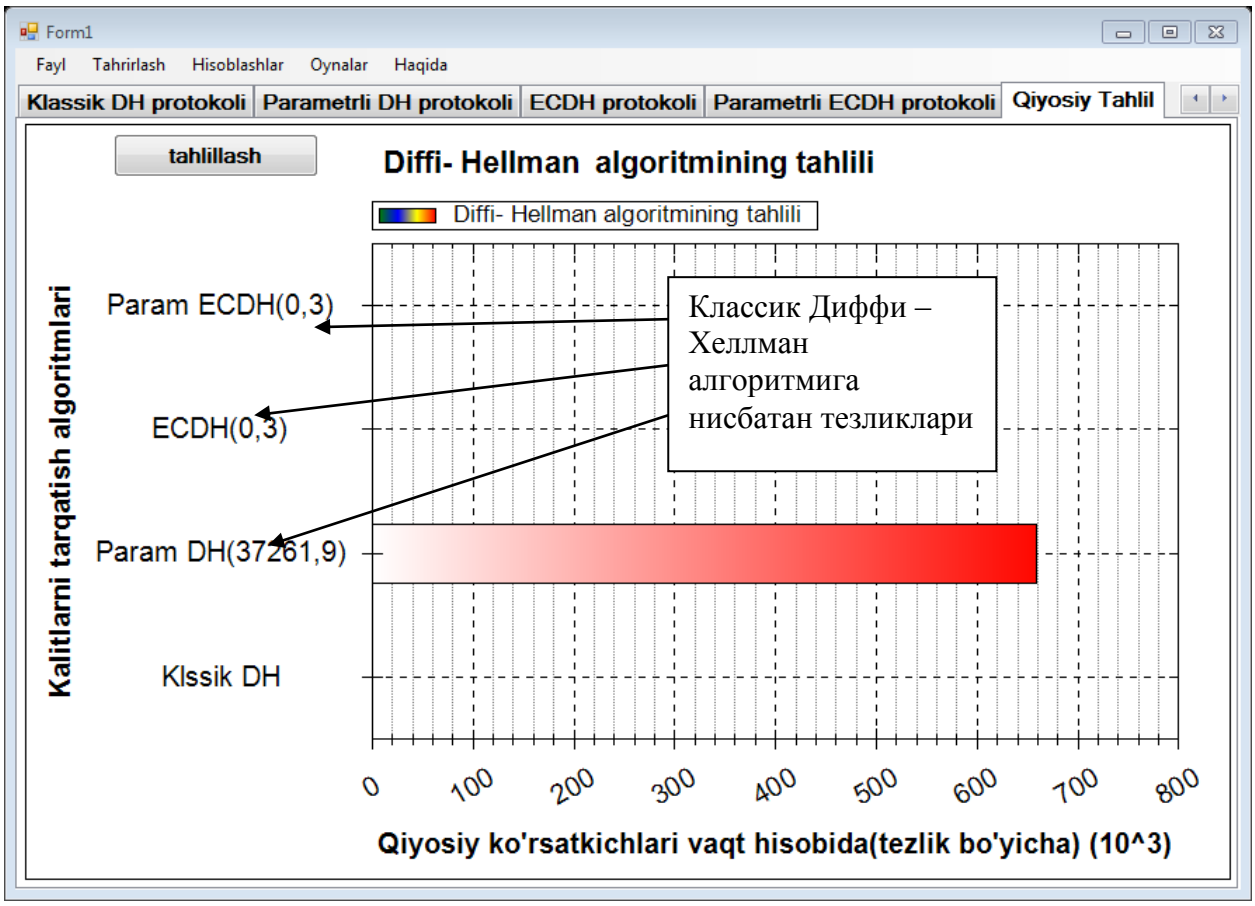
3.6. Параметрли алгебрага асосланган калитларни тақсимлаш алгоритмларининг қиёсий таҳлили

Қуйидаги ойнада Диффи–Хеллман алгоритмларининг тезлик (кичик сонларда) бўйича қиёсий таҳлили келтириб ўтилган (34-расм).



34-расм. Турли муаммолардаги Диффи-Хеллман алгоритмларининг тезлик (кичик сонларда) бўйича қиёсий таҳлили

35-расмда турли муаммоларга асосланган Диффи-Хеллман алгоритмларининг катта сонларда тезлиги бўйича қиёсий таҳлили тасвирланган. Қуйидага расм бўйича кўриниб турибдики, умумий параметрлар қанчалик катта бўлса катта сонларда ЭЭЧ ва ПЭЭЧ Диффи-Хеллман алгоритмлари тезкорлиги жуда юқори ҳисобланади.



35-расм. Турли муаммолардаги Диффи-Хеллман алгоритмларининг тезлик (катта сонларда) бўйича қиёсий таҳлили

Келтирилган графикда турли муаммоларга асосланган Диффи – Хеллман алгоритмларининг тезлиги бўйича таҳлил қилинди. Бу ердан кўриниб турибдики параметрли Диффи-Хеллман алгоритми бошқа муаммоларга нисбатан секин бажарилаяпти. Бунга сабаб даражага кўтариш жараёнида қўшимча R параметр ва даражага кўтаришнинг итерацион равишда босқичма-босқич ошиб боришидадир. Аммо криптобардошлик жиҳатидан классик Диффи-Хеллман алгоритмига нисбатан жуда яхши ҳисобланади. Параметрли Диффи-Хеллман алгоритмидан чекли сондаги оралиқларда фойдаланиш тавсия этилади.

Эллиптик эгри чизиқли ва параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман алгоритмлари эса классик алгоритмга нисбатан бироз секинроқ (34-расм), аммо етарлича катта сонларда классик Диффи–Хеллман алгоритмларидан тезкор ҳисобланади (35-расм). Бунга сабаб, етарлича катта сонларда даражага кўтариш жараёни мураккаблашса, эллиптик алгоритмларда қўшиш ва кўпайтириш амали орқали тезкорликка

эришилади. Бундан ташқари ЭЭЧ ва ПЭЭЧли Диффи-Хеллман алгоритмлари классик Диффи-Хеллман алгоритмига нисбатан юқори даражадаги криптобардошликка эга. Яъни ҳисоблаш жараёнлари калит алмашиш жараёнидан олдин бажарилганлиги ва қўшимча махфий параметрлар эвазига ПЭЭЧ алгоритми бошқа алгоритмларга нисбатан криптобардошлиги баланд ҳисобланади. Буни қуйидаги 7-жадвал орқали кўришимиз мумкин.

7-жадвал

Турли муаммолардаги Диффи-Хеллман алгоритмларининг қиёсий таҳлили

Алгоритм номи	**Диффи-Хеллман**	**Параметрли Диффи-Хеллман**	**Эллиптик эгри чизиқли Диффи-Хеллман**	**Параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман**
Муаммоси	Дискрет логармфмлаш	Параметрли алгебра	Эллиптик эгри чизиқли	Параметрли эллиптик эгри чизиқ
Мураккаблиги	содда	мураккаб	жуда мураккаб	жуда мураккаб
Тезлиги (кичик сонларда)	тезкор	6 марта секин	1.2 марта секинроқ	1.4 марта секинроқ
Тезлиги (катта сонларда)	3.5 марта секин	37262 марта секин	тезкор	тезкор
Умумий параметрлари	*g* - катта туб сон, *p* - катта туб сон модуль	*g* - катта туб сон, *p* - катта туб сон модуль, *R* - махфий параметр	*G(x,y)* – эллиптик эгри чизиқдаги нуқта, *p* - катта туб сон модуль, *n* - чекли майдон	*G(x,y)* – эллиптик эгри чизиқдаги нуқта, *p* - катта туб сон модуль, *n* - чекли майдон, *R* - махфий параметр
Амаллар сони	4 та даражага кўтариш, 4 та модуллаш	2 та даражага кўтариш, 4 та модуллаш, 8 та қўшиш, 4 та кўпайтириш	8 та модуллаш, 8 та кўпайтириш,	8 та модуллаш, 4 та кўпайтириш, 12 та қўшиш
Махфий параметрлари	*a* – **A** томон махфий калити, *b* – **B** томон махфий калити	*a* – **A** томон махфий калити, *b* – **B** томон махфий калити	*a* – **A** томон махфий калити, *b* – **B** томон махфий калити, *h, w, q*	*a* – **A** томон махфий калити, *b* – **B** томон махфий калити, *h, w, q*
Алгебраси	$Y=g^a(mod\ p)$	$Y=g^{\backslash a}(mod\ p)= a\Sigma_{i=0}^{i=a-1} F^i\ (mod\ p)$, *бу ерда* $F=1+Rg$	$y_0^2 \equiv x_0^3+ax_0+b\ (mod\ p)$, $Y=a*G(mod\ p)$,	$y^{\backslash 2} \equiv x^{\backslash 3}+ax+B\ (mod\ p)$, $Y=a*^{\backslash}G(mod\ p) =G+a+GaR(mod\ p)$

Қуйидаги 8-жадвалда турли муаммолардаги Диффи-Хеллман алгоритмларининг криптобардошлилиги баҳоси келтирилган.

8-жадвал

Турли муаммолардаги Диффи-Хеллман алгоритмларининг криптобардошлиги

Калитларни тақсимлаш алгоритмлари	**Махфий параметрлар**	**Параметр қийматлари (бит)**	**Криптобардошлик**
Классик Диффи-Хеллман	Махфий калит *x*	*512*	$I = 2^{847}$ бу ерда $I_x = 2^{80}$,
Параметрли Диффи-Хеллман	Махфий калит *x*, параметр *R*,	*512*, *512*	$I = 2^{847}$ бу ерда $I_x = 2^{80}$, $I_R = 2^{512}$
Эллиптик эгри чизиқли Диффи-Хеллман	Махфий калит d Параметрлар *a, B*	*512* (*q=512*, бу ерда *q* – бошланғич нуқтанинг тартиб рақами) 512, 512	$I_d = 2^{1027}$ $q = p4/\pi$ бу ерда $I_a = 2^{512}$, $I_B = 2^{512}$
Параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман	Махфий калит ***d*** Параметрлар *R, a, B*	*512*, *512, 512, 512,*	$I = 2^{1167}$ бу ерда $I_x = 2^{80}$, $I_R = 2^{512}$, $I_a = 2^{512}$, $I_B = 2^{512}$,

8-жадвалдан кўриниб турибдики, параметрга асосланган эллиптик эгри чизиқли Диффи-Хеллман калит тақсимлаш алгоритми бардошлилиги $I = 2^{1167}$ га тенг бўлиб, бошқа муаммоларга нисбатан юқори бардошли ҳисобланади. ПЭЭЧ калитларни тақсимлаш алгоритмларидан миллий электрон ҳужжат айланиш тизимларида фойдаланиш уларнинг муҳофазасини оширишга хизмат қилади. Бундан ташқари бу алгоритмдан кичик хотирадаги аппарат ва аппарат-дастурий воситаларда тезкор калитларни тақсимлашда фойдаланиш яхши ютуқларга олиб келади. ПЭЭЧ калитларни тақсилаш

алгоритмлари ҳимояланмаган телекоммуникаця тармоқларида калитларни хавфсиз, тезкор ҳамда криптобордош тарзда етказиб беришни таъминлайди. Бу алгоритм орқали хавфсиз, ҳимояланган алоқа канналари ва тизимларни ҳосил қилишда тезкорлиги, самарадорлиги ва криптобардошлигини кескин даражада кўтариш имкониятига ега бўламиз. Бундан келиб чиқиб, ПЭЭЧ калитларни тақсимлаш алгоритми ҳозирги замон талабларига тўлиқ жавоб бера оладиган тизимларни қуришда фойдаланиш мақсадга мувофиқ ҳисобланади.

Ишлаб чиқилган дастурларнинг коди иловада келтирилди.

3-боб бўйича хулосалар

1. Носимметрик криптографиянинг математик асоси бўлиб бирор алгебраик структура ва унда криптографик алгоритмга асос қилиб олинган яширин йўлли бир томонлама функция хизмат қилишини инобатга олган ҳолда бу бобда эллиптик эгри чизиқли алгоритмларни параметрли кўринишга ўтказиш усули таҳлил қилиб чиқилди.

2. Параметрли Диффи-Хеллман калит алмашиш алгоритмини ишлаб чиқиш усули келтирилди. 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.

3. Параметрли эллиптик эгри чизиққа асосланган Диффи-Хеллман калит алмашиш алгоритми эллиптик эгри чизиқли Диффи-Хеллман алгоритмига нисбатан криптобардошлиги юқори бўлиши кўрсатилди.

4. Диффи-Хеллман калитларни тақсимлаш алгоритми асосида дастурий таъминот ишлаб чиқилди ва AES шифрлаш алгоритми асосида фойдаланувчилар ўртасида мулоқот жараёни кўрсатиб берилди.

5. Эллиптик эгри чизиқли ва параметрли Диффи-Хеллман алгоритмлари асосида дастурий таъминот яратилиб, эллиптик эгри чизиқли параметрли алгебрага асосланган калитларни тақсимлаш алгоритмларининг тезлиги ва криптобардошлиги бўйича қиёсий таҳлил натижалари келтирилди.

ХУЛОСА

Магистрлик диссертацияси ишини бажариш жараёнида қуйидаги асосий натижалар олинди:

1. Криптотизимлардан фойдаланиш жараёнлари калитларни бошқариш жараёнлари масалалари билан боғлиқлигигини асослаган ҳолда криптографик калитларни тақсимлашнинг замонавий усуллари ва схемалари тадқиқ этилди.

2. Носимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколларидан ҳужжатли маълумотларнинг махфийлигини таъминлаш учун фойдаланиш мумкинлиги изоҳланди.

3. Ҳозирги кунда ишлаб чиқилган элиптик эгри чизиқлардан фойдаланишга асосланган калитларни тақсимлаш тизимларининг анъанавий тизимларга нисбатан афзаллиги, уларда фойдаланиладиган калит узунлиги разряди кичик бўлганда ҳам, эквивалент ҳимоя билан таъминлашидадир. Бу эса қабул қилувчи ва узатувчи мослама процессорларининг юкланиш вақтини камайтириши изоҳланди.

4. Эллиптик эгри чизиқли калит тақсимлаш алгоритмларининг криптобардошлиги жуда мураккаб деб тан олинган масала - эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблигига асосланган бўлиб, уларнинг бардошлигини оширишнинг ҳозирги кундаги энг самарали усули ЭЭЧ базавий нуқталари тартиби q ни ошириш усули эканлиги кўрсатилди.

5. Носимметрик криптографиянинг математик асоси бўлиб бирор алгебраик структура ва унда криптографик алгоритмга асос қилиб олинган яширин йўлли бир томонлама функция хизмат қилишини инобатга олган ҳолда эллиптик эгри чизиқли алгоритмларни параметрли кўринишга ўтказиш усули таҳлил қилиб чиқилди.

6. Эллиптик эгри чизиқли алгоритмларни параметрли кўринишга ўтказиш усули асосида параметрли эллиптик эгри чизиққа асосланган Диффи-Хеллман калит алмашиш алгоритми ишлаб чиқилди.

7. Диффи-Хеллман калитларни тақсимлаш алгоритми асосида дастурий таъминот ишлаб чиқилди ва AES шифрлаш алгоритми асосида фойдаланувчилар ўртасида мулоқот жараёни кўрсатиб берилди.

8. Эллиптик эгри чизиқли ва параметрли Диффи-Хеллман алгоритмлари асосида дастурий таъминот яратилиб, эллиптик эгри чизиқли

параметрли алгебрага асосланган калитларни тақсимлаш алгоритмларининг тезлиги ва криптобардошлиги бўйича қиёсий таҳлил натижалари келтирилди.

9. Параметрли эллиптик эгри чизиқли Диффи-Хеллман алгоритми криптобардошлик ва тезлик жиҳатидан бошқа муммолардаги Диффи-Хеллман алгоритмларидан устун ҳисобланади ва бу алгоритмдан криптобардошлиги ва тезлиги юқори бўлган миллий калитларни тақсимлаш стандартида фойдаланиш тавсия этилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. «Ахборотлаштириш тўғрисида»ги Ўзбекистон Республикаси Қонуни. 11.12.2003 й. №560-II.

2. «Ўзбекистон Республикасида ахборотнинг криптографик муҳофазасини ташкил этишга доир чора-тадбирлари тўғрисида» ги Ўзбекистон Республикаси Президентининг ПҚ-614-сон қарори. – Тошкент, 3 апрел 2007 йил.

3. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

4. Винокуров А. Современность практической криптографии // Системы безопасности связи и телекоммуникаций. – 2003. – №10. – С. 218-221.

5. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005. – 768 с.

6. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

7. Зензин О., Иванов М. Стандарт криптографической защиты – AES. Конечные поля. – Изд.:Кудиц - Образ, 2002. – 176 с.

8. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008. – 382 б.

9. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. - Изд.: Лори Гелиос АРВ, 2002.- 240 с.

10. Diffie, W., Hellman, M. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

11.Чмора А.Л. Современная прикладная криптография. Изд.:Гелиос, 2001.- 256 с.

12. Акбаров Д.Е. «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» - Т.: «Ўзбекистон маркаси», 2009. - 424 б.

13. 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.

14. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). – Pp. 173-193.

15. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. – Pp. 203-209.

16. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988. – 320 с.

17. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002. – 816 с.

18. Нильс Фергюсон, Брюс Шнайер. Практическая криптография – Москва: "Диалектика", 2004. – 432 с.

19. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - Изд.:Лори Гелиос АРВ, 2005.- 192 с.

20. US Patent, Hellman, et al. Cryptographic apparatus and method, 4.200.770, April 29, 1980.

21. US Patent, Rivest R., Shamir A. and Adleman L.: Cryptographic Communications System and Method. 4,405,829, 1983.

22. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Учебное пособие. - Изд.:Лори Горячая Линия - Телеком, 2002.- 175 с.

23. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – Изд.:МЦНМО, 2003. – 328 с.

24. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. – 780 pp.

25. Alfred J. Menezes: Elliptic curve public key cryptosystems, Kluwer academic publishers, 1993. – 152 pp.

26. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.-456 pp.

27. Ященко В.В. Криптография, раньше была засекречена // ”Компьютера”, 1998, №20.- 250 с.

28. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. - Санкт-Петербург, 2004. – 106 с.

29. Масленников М., Практическая криптография. - М.:Лори BHV - Санкт - Петербург, 2003.- 464 с.

30. Шнайер Б. Слабые места криптографических систем // Открытые системы. – 1999, № 1. – С. 31-36.

31. Стахов А.П. «ЗОЛОТАЯ» КРИПТОГРАФИЯ, Таганрог http://www.goldenmuseum.com/ http://www.trinitas.ru/rus/

32. Shamir, A. On the generation of cryptographically strong pseudo-random sequences // ACM Transactions on Computer Systems, vol. 1, 1983. – Pp. 38-44.

33. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Advances in Cryptology — CRYPTO ’90. LNCS. Springer–Verlag. 1991. V. 537. P.

34. Hellman M. A cryptanalytic time-memore trade-off // IEEE Transactionson Information Theory, vol. IT-26, 1980. – Pp. 401-406.

35. Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. // http://citeseer.ist.psu.edu - Cryptography Research, Inc., San Francisco, USA. Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT ’93. 1994. LNCS. Springer–Verlag. V. 765. P.

36. Menezes A.J. Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

37. Min-Shiang Hawng, Cheng-Chi Le. Research issues and challenges for multiple digital signature // Int. J. of Network Security. – 2005. – Vol. 1, No 1. – P. 1–7.

38.Молдовян Н.А., Молдовян П.А. Новые протоколы слепой подписи // Безопасность информационных технологий. – М.:МИФИ. –2007. – № 3. – С. 17–21

39.ISO/IEC 11770 -1. “Key management – Introduction”.

40.ISO/IEC 11770 -2. “Key management – Symmetric techniques”.

41.ISO/IEC 11770 -3. “Key management – Asymmetric techniques”.

42.The Secure Sockets Layer Protocol. http://www.netscape.com/info/security-doc.html.

43. El Gamal T. A Public-key Cryptosystem and a Signature Based onDiscrete Logarithms. IEEE Trans. Inform. Theory, Vol. IT-31,pp.469-472, July 1985.

44. "Digital Signature Standard (DDS)", Federal Information Processing Standards Publication 186, May 19, 1994, pp.1-18.

45. 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).

46. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000).

47. Алферов А.П., Зубов А.К., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. - 2-е изд., испр. и доп. — М.. Гелиос АРВ, 2002. — 480 с.

48. Фомичев В.М. Дискретная математика и криптология. Курс лекций. -М., Диалог-МИФИ, 2003. - 400 с.

49. Бабаш А.В., Шанкин Г.П. Криптография. Под редакцией В.П. Шерстюка, ЭЛ. Применко / А.В. Бабаш, Г.П. Шанкин. - М.: СОЛОН-ПРЕСС, 2007. - 512 с. - (Серия книг «Аспекты защиты»). ISBN 5-93455-135-3

50. Панасенко С. Алгоритмы шифрования. Специальный справочник. - СПб: БХВ-Петербург, 2009 г., 576 с.

51. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические н алгоритмические основы. — М.: КомКнига, 2006. — 328 с.

52. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых.. - М.: Изд. КомКнига, 2006, 328 стр.

53. Острик В.В., Цфасман М.А. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые - М.: МЦНМО, 2001.— 48 с. (Библиотека "Математическое просвещение", выпуск 8).

Дастур коди

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using ZedGraph;
using System.Numerics;
using System.Diagnostics;
using System.Threading;

namespace Ecni_hisoblash
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
            this.StartPosition = FormStartPosition.CenterScreen;
        }

        #region O'zgaruvchilar qismi
        public List<int> result = new List<int> { };
        public void tubchalar(int i)
        {
            result.Add(i);
        }
        double y, z;
        string aa = "";
        int p, jj = 0;
        private void cbxTuldir()
        {
            for (int i = -800; i < 800; i++)
            {
                cbxA.Items.Add(i);
                cbxB.Items.Add(i);
                if(i>5)
                cbxN.Items.Add(i);
            }
            cbxA.SelectedItem =Convert.ToInt32(publicParam.publicA);
            cbxB.SelectedItem = Convert.ToInt32(publicParam.publicB);
            cbxN.SelectedItem = Convert.ToInt32(publicParam.publicN);

        }
        PublicParametrs publicParam = new PublicParametrs();

        #endregion

        private string ishoracha(int l)
        {
            string result = string.Empty;
            return l>0? result = "+":result;
        }
        #region Grafik qurish qismi
        public void GrafBuild(int aa, int bb, int nn)
        {
```

```
            jj = 0;
            double[] xx, yy;
           double zz=0;
             List<double> listX=new List<double>{};
             List<double> listY=new List<double>{};

            Grafik.GraphPane.CurveList.Clear();


                lblTenglama.Text = "Y^2 = X^3 " +ishoracha(aa)+" " + aa.ToString() + " *
X " +ishoracha(bb) +" "+ bb.ToString();
            // GraphPane object holds one or more Curve objects (or plots)

            GraphPane myPane = Grafik.GraphPane;
            for (double i = -nn; i < nn; i+=0.1)
            {

                 zz= System.Math.Sqrt(System.Math.Pow(i, 3)-aa*i+bb);

                     listX.Add(i);
                     listY.Add(zz);
                     jj++;

            }
            for (double i = -nn; i < nn; i +=0.1)
            {

               zz = -System.Math.Sqrt(System.Math.Pow(i, 3) -aa*i+bb );

                    listX.Add(i);
                    listY.Add(zz);
                    jj++;

            }
            yy = new double[listY.Count-1];
            xx = new double[listX.Count-1];
            for (int i = 0; i < yy.Length; i++)
            {
                yy[i] = listY[i+1];
                xx[i] = listX[i+1];
            }

            PointPairList spl1 = new PointPairList(xx, yy);

            LineItem EgriChiziq = myPane.AddCurve("Elliptik egri chiziq", spl1,
Color.Green, SymbolType.None);

            EgriChiziq.Line.Width = 3.0F;

            myPane.Title.Text = "Elliptik Egri chiziq grafigi";
            myPane.YAxis.Title.Text = "Y qiymatlar sohasi";
            myPane.XAxis.Title.Text = "X aniqlanish sohasi";
            Grafik.AxisChange();
            Grafik.Invalidate();
            Grafik.Refresh();

        }
        #endregion

        #region Optimal ECC ni aniqlash berilgan A va B oraliqda
        private string OptimalECC(string nn)
        {
            int a = 10, b = 10, x = 0, k = 0;
            string resultText = string.Empty;
            int n = Convert.ToInt32(nn);
```

```
            p = n;
            //musbatlari
            for (int l = -a; l < a; l++)  // A bu yerda l
            {
                for (int s = -b; s < b; s++) // B bu yerda l
                {
                    x = 0;
                    if (4 * System.Math.Pow(l, 3) + 27 * System.Math.Pow(s, 2) % p != 0)
                    {
                        resultText += "\r\n\t\t\t A= " + l + "\t\tB=" + s + "\r\n";
                        for (int i = 0; i < n; i++)
                        {
                            y = System.Math.Sqrt(System.Math.Pow(i, 3) - l * i + s);
                            z = System.Math.Ceiling(y);
                            if (y == z)
                            { resultText += "C[" + i + "](" + i + " , " + y + ")    ";
x++; }
                        }
                    }
                    else
                    {

                    }
                    if (k < x)
                    {
                        k = x;
                        aa = "\nA=" + l + "\tB=" + s + "\t\tN=" + n + " oraliqdagi
yechimlar soni H= " + k + " ta buldi. Bu yechim shu oraliqda optimal hisoblandi.";
                        publicParam.publicA = l.ToString();
                        publicParam.publicB = s.ToString();
                        publicParam.publicN = n.ToString();
                        //ff = l + "," + s + "," + n;
                    }

                }
            }
            resultText += "\r\n\t\t\t HisoblashTugatildi!!!";
            resultText += "r\n\n\t\t\t********** \r" + aa;
            return resultText;
        }
        #endregion

        private void button1_Click(object sender, EventArgs e)
        {

            richTextBox1.Clear();
            richTextBox1.Text = OptimalECC(textBox1.Text);
            cbxTuldir();
        }

        private void button2_Click(object sender, EventArgs e)
        {
           //mm = ff.Split(',');
            int qa = Convert.ToInt32(publicParam.publicA);
            int qb = Convert.ToInt32(publicParam.publicB);
            int qn;
            if(cbxN.SelectedIndex>0)
                qn=Convert.ToInt32(cbxN.SelectedItem);
            else
             qn = Convert.ToInt32(publicParam.publicN);
            if (4 * System.Math.Pow(qa, 3) + 27 * System.Math.Pow(qb, 2) % p != 0)
            GrafBuild(qa, qb, qn);
        }

        private void cbxA_SelectedIndexChanged(object sender, EventArgs e)
```

```
        {
            int aaa =Convert.ToInt32(cbxA.SelectedItem);
           publicParam.publicA =Convert.ToString(aaa);
            int bbb = Convert.ToInt32(publicParam.publicB);
            lblTenglama.Text = "Y^2 = X^3 " + ishoracha(aaa) + " " + aaa.ToString() + " *
X " + ishoracha(bbb) + " " + bbb.ToString();
        }

        private void cbxB_SelectedIndexChanged(object sender, EventArgs e)
        {
            int bbb = Convert.ToInt32(cbxB.SelectedItem);
            publicParam.publicB = Convert.ToString(bbb);
            int aaa = Convert.ToInt32(publicParam.publicA);
            lblTenglama.Text = "Y^2 = X^3 " + ishoracha(aaa) + " " + aaa.ToString() + " *
X " + ishoracha(bbb) + " " + bbb.ToString();
        }

        private void cbxN_SelectedIndexChanged(object sender, EventArgs e)
        {

        }

        private void tubSonlarRoyxatiToolStripMenuItem_Click(object sender, EventArgs e)
        {
            Tub_sonlar tub = new Tub_sonlar();
            tub.f1 = this;
            tub.Show();
        }

        private void tubSonlarRoyxatiToolStripMenuItem_Click_1(object sender, EventArgs
e)
        {

        }

        #region Pni tekshirish
        private void PniTekshir()
        {
            richDescription.Clear();
            if (result.Count > 2)
            {
                if (!string.IsNullOrEmpty(txtP.Text))
                {
                    int p = int.Parse(txtP.Text);
                    if (!result.Contains(p))
                    {
                        richDescription.ForeColor = Color.Red;
                        richDescription.Text += "P= " + p + " tub son bo'lishi  kerak
\r\n Shart bajarilmadi\r\n.";
                    }
                    else
                    {
                        richDescription.ForeColor = Color.Green;
                        richDescription.Text += "P= " + p + " tub son  \r\n Shart
bajarildi\r\n.";
                    }
                }
            }
            else
            {
                richDescription.ForeColor = Color.Red;
                richDescription.Text += "Iltimos HISOBLASHLAR menyusidan tub sonlar
ro'yxati hisoblang";
            }
        }
```

```
        #endregion

        #region AniTekshir

        private void AniTekshir()
        {
            if (!string.IsNullOrEmpty(txtA.Text) && !string.IsNullOrEmpty(txtP.Text))
            {
                int a = int.Parse(txtA.Text);
                int p = int.Parse(txtP.Text);
                richDescription.ForeColor = Color.Black;
                richDescription.Text += "\r\n a mod p <> 0 shart ni tekshirish:\r\n";
                if (a % p == 0)
                {
                    richDescription.ForeColor = Color.Red;
                    richDescription.Text += a + " mod " + p + " = " + a % p + " \r\n
Shart bajarilmadi\r\n.";
                }
                else
                {
                    richDescription.ForeColor = Color.Green;
                    richDescription.Text += a + " mod " + p + " = " + a % p + " \r\n
Shart bajarildi\r\n.";
                }
            }
            else
            {
                richDescription.ForeColor = Color.Red;
                richDescription.Text +=  "P va A ni kiriting";
            }
        }
        #endregion

        #region BniTekshir

        private void BniTekshir()
        {
            if (!string.IsNullOrEmpty(txtB.Text) && !string.IsNullOrEmpty(txtP.Text) &&
!string.IsNullOrEmpty(txtA.Text))
            {
                int b = int.Parse(txtB.Text);
                int p = int.Parse(txtP.Text);
                int a = int.Parse(txtP.Text);
                richDescription.ForeColor = Color.Black;
                richDescription.Text += "\r\n a mod p <> 0 shart ni tekshirish:";
                if (b % p == 0)
                {
                    richDescription.ForeColor = Color.Red;
                    richDescription.Text += "\r\n" + b + " mod " + p + " = " + b % p + "
\r\n Shart bajarilmadi. \r\n";
                }
                else
                {
                    richDescription.ForeColor = Color.Green;
                    richDescription.Text += "\r\n" + b + " mod " + p + " = " + b % p + "
\r\n Shart bajarildi. \r\n";
                }
                richDescription.Text +="\r\n 4*a^3 +27*b^2<>0 (mod p) shartni
tekshirish:";
                if ((4 * a * a * a + 27 * b * b) % p != 0)
                {
                    richDescription.ForeColor = Color.Green;
                    richDescription.Text += "\r\n4 *" + a + "^3 + 27 * " + b + "^2=" + (4
* a * a * a + 27 * b * b) % p + " (mod " + p + ") \r\n Shart bajarildi\r\n.";
```

```
                }
                else
                {
                    richDescription.ForeColor = Color.Red;
                    richDescription.Text += "\r\n4 *" + a + "^3 + 27 * " + b + "^2=" + (4
* a * a * a + 27 * b * b) % p + " (mod " + p + ") \r\n Shart bajarilmadi\r\n.";
                }

            }
            else
            {
                richDescription.ForeColor = Color.Red;
                richDescription.Text += Environment.NewLine + "P, B va A ni kiriting";
            }
        }
        #endregion

        #region  Q va W ni tekshirish
        private void qw()
        {
            int p = int.Parse(txtP.Text);
            int p1 = p + 1 - 2 * Convert.ToInt32(System.Math.Sqrt(p));
            int p2 = p + 1 + 2 * Convert.ToInt32(System.Math.Sqrt(p));
            int w = rn.Next(p1, p2);
            txtW.Text = w.ToString();
            txtH.Text = rn.Next(3, 30).ToString();
            richDescription.Text += "\r\n p+1-2*sqrt(p) < w < p+1+2*sqrt(p) oraliqqa
tekshirish:\r\n";
            richDescription.Text += +p1 + " < " + w + " <" + p2 + "oraliqqa kiradi:\r\n";

            int indexTub = rn.Next(result.Count / 2, result.Count);
            txtG.Text = result[indexTub].ToString();
            richDescription.Text += "\r\n G ni tublikka tekshirish:\r\n";
            richDescription.Text += result[indexTub] + " =tub son\r\n";
            int indexR = rn.Next(result.Count / 2, result.Count);
            txtR.Text = result[indexR].ToString();
            richDescription.Text += "\r\n R maxfiy parametrni qabul qilish:\r\n";
            richDescription.Text += result[indexR] + "= maxfiy parametr qabul
qilindi\r\n";
        }
        #endregion

        private void txtP_TextChanged(object sender, EventArgs e)
        {
            if (!string.IsNullOrEmpty(txtA.Text) && !string.IsNullOrEmpty(txtB.Text) &&
!string.IsNullOrEmpty(txtP.Text))
                button3.Enabled = true;
            else
                button3.Enabled = false;
            PniTekshir();
        }

        private void txtA_TextChanged(object sender, EventArgs e)
        {
            if (!string.IsNullOrEmpty(txtP.Text) && !string.IsNullOrEmpty(txtB.Text) &&
!string.IsNullOrEmpty(txtA.Text))
                button3.Enabled = true;
            else
                button3.Enabled = false;
            PniTekshir();
            AniTekshir();
        }

        private void txtB_TextChanged(object sender, EventArgs e)
        {
```

```
            if (!string.IsNullOrEmpty(txtA.Text) && !string.IsNullOrEmpty(txtP.Text) &&
!string.IsNullOrEmpty(txtB.Text))
                button3.Enabled = true;
            else
                button3.Enabled = false;
            PniTekshir();
            AniTekshir();
            BniTekshir();
        }

        private void txtP_KeyPress(object sender, KeyPressEventArgs e)
        {
            if (char.IsLetter(e.KeyChar) ||
         char.IsSymbol(e.KeyChar) ||
         char.IsWhiteSpace(e.KeyChar) ||
         char.IsPunctuation(e.KeyChar))
                e.Handled = true;
        }
        Random rn = new Random();
        private void button3_Click(object sender, EventArgs e)
        {

            bool tek=true;
            int i = 0;
            int b = int.Parse(txtB.Text);
            int p = int.Parse(txtP.Text);
            int a = int.Parse(txtA.Text);
            while(tek)
            {
                y = System.Math.Sqrt(System.Math.Pow(i, 3) + a * i + b)%p;
                z = System.Math.Ceiling(y);
                if (y == z)
                { txtGX.Text = i.ToString(); txtGY.Text = y.ToString(); tek = false; }
                i++;
            }
            txtN.Text = result[result.Count/2].ToString();
            PniTekshir();
            AniTekshir();
            BniTekshir();
             richDescription.ForeColor = Color.Green;
             richDescription.Text += string.Format("\r\nG(X,Y)=({0},{1})  Elliptik egri
chiziqqa tegishli bo'lgan nuqta.\r\n\r\n Berilgan oraliqdagi elliptik egri chiziq\n
yechimlari soni N={2} ta\r\n", txtGX.Text, txtGY.Text,txtN.Text);
             qw();
        }

        private void kattaTubSonHosilQilishToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Katta_Tub_Son frmcha = new Katta_Tub_Son();
            frmcha.Show();
        }
        ParametrliAlgebra pr = new ParametrliAlgebra();
        private void bosqich1(int indexA)
        {
            int p = int.Parse(txtP.Text);
            int g = int.Parse(txtG.Text);
            if (indexA == 0)
             indexA = rn.Next(p/2,p);
            txtAmaxfiy.Text = indexA.ToString();
            int Ajunat = pr.daraja(g, indexA, p);
            txtAjunat.Text = Ajunat.ToString();
            lblbosqich1.ForeColor = Color.DarkGreen;

        }
```

```
private void bosqich2(int indexb)
{
    int p = int.Parse(txtP.Text);
    int g = int.Parse(txtG.Text);
    if (indexb == 0)
    indexb = rn.Next(p / 2, p);
    txtBmaxfiy.Text = indexb.ToString();
    int Bjunat = pr.daraja(g, indexb, p);
    txtBjunat.Text = Bjunat.ToString();
    lblbosqich2.ForeColor = Color.DarkGreen;

}
private void bosqich3()
{

    int p = int.Parse(txtP.Text);
    int g = int.Parse(txtG.Text);
    int A = int.Parse(txtAjunat.Text);
    int B = int.Parse(txtBjunat.Text);
    int a = int.Parse(txtAmaxfiy.Text);
    int b = int.Parse(txtBmaxfiy.Text);
    int Ka = pr.daraja(B, a, p);
    int Kb = pr.daraja(A, b, p);
    txtKa.Text = Ka.ToString();
    txtKb.Text = Kb.ToString();
    lblKumumiy.ForeColor = Color.DarkGreen;
    lblKumumiy.Text = "K=Ka=Kb";

}

private void button10_Click(object sender, EventArgs e)
{
    bosqich1(0);
}

private void button4_Click(object sender, EventArgs e)
{
    bosqich2(0);
}

private void button6_Click(object sender, EventArgs e)
{
    bosqich3();
}

private void lblKumumiy_Click(object sender, EventArgs e)
{

}

private void button15_Click(object sender, EventArgs e)
{
    txtgklassik.Text = txtG.Text;
    txtpKlassik.Text = txtP.Text;
}

private void button26_Click(object sender, EventArgs e)
{
    txtgP.Text = txtG.Text;
    txtpP.Text = txtP.Text;
    txtrR.Text = txtR.Text;
}
private void parambosqich1(int indexA)
{
    int p = int.Parse(txtP.Text);
```

```
            int g = int.Parse(txtG.Text);
            int R = int.Parse(txtR.Text);
            if(indexA==0)
             indexA = rn.Next(p / 2, p);
            txtAMaxP.Text = indexA.ToString();
            double Ajunat = pr.daraja(g, indexA, p,R);
            txtAjunatP.Text = Ajunat.ToString();
            lblbosqich1P.ForeColor = Color.DarkGreen;
        }
        private void parambosqich2(int indexb)
        {
            int p = int.Parse(txtP.Text);
            int g = int.Parse(txtG.Text);
            int R = int.Parse(txtR.Text);
              if(indexb==0)
                  indexb = rn.Next(p / 2, p);
            txtBMaxP.Text = indexb.ToString();
            double Bjunat = pr.daraja(g, indexb, p,R);
            txtBjunatP.Text = Bjunat.ToString();
            lblbosqich2P.ForeColor = Color.DarkGreen;
        }
        private void parambosqich3()
        {
            int p = int.Parse(txtP.Text);
            int g = int.Parse(txtG.Text);
            int A = int.Parse(txtAjunatP.Text);
            int B = int.Parse(txtBjunatP.Text);
            int a = int.Parse(txtAMaxP.Text);
            int b = int.Parse(txtBMaxP.Text);
            int R = int.Parse(txtR.Text);
            double Ka = pr.daraja(B, a, p,R);
            double Kb = pr.daraja(A, b, p,R);
            txtKaP.Text = Ka.ToString();
            txtKbP.Text = Kb.ToString();
            lblnatP.ForeColor = Color.DarkGreen;
            lblnatP.Text = "K=Ka=Kb";
            lblum.ForeColor = Color.DarkGreen;
        }

        private void button25_Click(object sender, EventArgs e)
        {
            parambosqich1(0);
        }

        private void button23_Click(object sender, EventArgs e)
        {
            parambosqich2(0);
        }

        private void button18_Click(object sender, EventArgs e)
        {
            parambosqich3();
        }

        private void label63_Click(object sender, EventArgs e)
        {

        }

        private void button38_Click(object sender, EventArgs e)
        {
            lblecdhteng.Text = "Y^2 = X^3 +" + txtA.Text + " *X +" + txtB.Text + "mod ("
+ txtP.Text + ")";
            txtPecdh.Text = txtP.Text;
            txtXecdh.Text = txtGX.Text;
```

```
    txtYecdh.Text = txtGY.Text;
}
private void bosqichecdh1(int a)
{

    int p =int.Parse(txtP.Text);
    int x = int.Parse(txtGX.Text);
    int y = int.Parse(txtGY.Text);
    if(a==0)
     a = rn.Next(p / 2, p);
    txtaECDH.Text = a.ToString();
    a %= p;
    double ax = ((x % p) *a )% p;
    double ay = ((y % p) * a) % p;
    txtAjECDH.Text = ax + "," + ay;
    lblecdh1.ForeColor = Color.DarkGreen;

}
private void bosqichecdh2(int b)
{

    int p = int.Parse(txtP.Text);
    int x = int.Parse(txtGX.Text);
    int y = int.Parse(txtGY.Text);
    if(b==0)
     b = rn.Next(p / 2, p);
    txtbECDH.Text = b.ToString();
    b %= p;
    double bx = ((x % p) * b) % p;
    double by = ((y % p) * b) % p;
    txtBjECDH.Text = bx + "," + by;
    lblecdh2.ForeColor = Color.DarkGreen;
}
private void bosqichecdh3()
{

    int a = int.Parse(txtaECDH.Text);
    int b = int.Parse(txtbECDH.Text);
    int p = int.Parse(txtP.Text);
    string AXY = txtAjECDH.Text;
    string[] xy = AXY.Split(',');
    int ax = int.Parse(xy[0]);
    int ay = int.Parse(xy[1]);

    string BXY = txtBjECDH.Text;
    string[] xyb = BXY.Split(',');
    int bx = int.Parse(xyb[0]);
    int by = int.Parse(xyb[1]);

    a %=p; b %=p;
    double Kax=((bx%p)*a)%p; double Kay=((by%p)*a)%p;
    int Kbx=((ax%p)*b)%p;int Kby=((ay%p)*b)%p;
    txtKaCDH.Text = string.Format("{0},{1}", Kax, Kay);
    txtKbCDH.Text = (Kbx + "," + Kby).ToString();
    lblecdhnat.ForeColor = Color.DarkGreen;
    lblecdhnat.Text = "K=Ka=Kb";

}

private void btnesdh1_Click(object sender, EventArgs e)
{
    bosqichecdh1(0);
}

private void btnecdh2_Click(object sender, EventArgs e)
```

```
        {
            bosqichecdh2(0);
        }

        private void btnecdh3_Click(object sender, EventArgs e)
        {
            bosqichecdh3();
        }

        private void chiqishToolStripMenuItem_Click(object sender, EventArgs e)
        {
            this.Close();
        }

        private void P_ECDH_function()
        {
            int a  =int.Parse(txtA.Text);
            int b = int.Parse(txtB.Text);
            int p = int.Parse(txtP.Text);
            int r = int.Parse(txtR.Text);
            int i = 0;
            bool tek = true;
            double y2,yP2;
            b = (a + b) * r % p;
            while (tek)
            {
                i = rn.Next(p / 2, p);
                y2 = (System.Math.Pow(i, 3) + a * i + b) % p;
                yP2 = (y2 - 1) * r % p;
                z = System.Math.Ceiling(yP2);
                if (yP2 == z)
                { txtPecdhX.Text = i.ToString(); txtPecdhY.Text = yP2.ToString(); tek =
false; }
                i++;
            }
            lblPecdhteng.Text = "Y^\\2 = X^\\3 +" + txtA.Text + " *X +" + b + "mod (" +
txtP.Text + ")";

        }

        private void button29_Click(object sender, EventArgs e)
        {

            txtPecdhP.Text = txtP.Text;
            txtPecdhR.Text = txtR.Text;
            P_ECDH_function();

        }
        private void bosqichPecdh1(int a)
        {

            int p = int.Parse(txtP.Text);
            int x = int.Parse(txtPecdhX.Text);
            int y = int.Parse(txtPecdhY.Text);
            int r = int.Parse(txtR.Text);
            if (a == 0)
                a = rn.Next(p / 2, p);
            txtPecdhA.Text = a.ToString();
            a %= p;
            x %= p;
            y %= p;
            double ax = pr.kupaytirish(x,a,p,r);
            double ay = pr.kupaytirish(y, a, p, r);
            txtPecdhPa.Text = ax + "," + ay;
            label78.ForeColor = Color.DarkGreen;
```

```
        }
        private void bosqichPecdh2(int b)
        {

            int p = int.Parse(txtP.Text);
            int x = int.Parse(txtGX.Text);
            int y = int.Parse(txtGY.Text);
            int r = int.Parse(txtR.Text);
            if (b == 0)
                b = rn.Next(p / 2, p);
            txtPecdhB.Text = b.ToString();
            b %= p;
            x %= p;
            y %= p;
            double bx = pr.kupaytirish(x, b, p, r);
            double by = pr.kupaytirish(y, b, p, r);
            txtPecdhPb.Text = bx + "," + by;
            label28.ForeColor = Color.DarkGreen;
        }
        private void bosqichPecdh3()
        {

            int a = int.Parse(txtPecdhA.Text);
            int b = int.Parse(txtPecdhB.Text);
            int p = int.Parse(txtP.Text);
            int r = int.Parse(txtR.Text);
            string AXY = txtPecdhPa.Text;
            string[] xy = AXY.Split(',');
            int ax = int.Parse(xy[0]);
            int ay = int.Parse(xy[1]);

            string BXY = txtPecdhPb.Text;
            string[] xyb = BXY.Split(',');
            int bx = int.Parse(xyb[0]);
            int by = int.Parse(xyb[1]);

            a %= p; b %= p;
            bx %= p; by %= p; ay %= p; ax %= p;
            double Kax = pr.kupaytirish(bx, a, p, r); double Kay = pr.kupaytirish(by, a,
p, r);
            double Kbx = pr.kupaytirish(ax, b, p, r); double Kby = pr.kupaytirish(ay, b,
p, r);
            txtPecdhKa.Text = string.Format("{0},{1}", Kax, Kay);
            txtPecdhKb.Text = string.Format("{0},{1}", Kax, Kay);
            lblecdhPNat.ForeColor = Color.DarkGreen;
            lblecdhPNat.Text = "K=Ka=Kb";

        }
        private void button44_Click(object sender, EventArgs e)
        {
            bosqichPecdh1(0);
        }

        private void btntahlil_Click(object sender, EventArgs e)
        {
            buildGraph();
        }



        #region Grafik regioni

        #region Kontext menyu
```

```
        void Grafik_ContextMenuBuilder(ZedGraphControl sender,
          ContextMenuStrip menuStrip,
          Point mousePt,
          ZedGraphControl.ContextMenuObjectState objState)
        {

            menuStrip.Items[0].Text = "Nusxa ko'chirish";
            menuStrip.Items[1].Text = "Gistogrammani boshqa nomda saqlash";
            menuStrip.Items[2].Text = "Sahifa parametrlari…";
            menuStrip.Items[3].Text = "Bosmaga chiqarish…";
            menuStrip.Items[4].Text = "Nuqta qiymatlarini ko'rsatish…";
            menuStrip.Items[7].Text = "Standart masshtabni tanlash...";

            menuStrip.Items.RemoveAt(5);
            menuStrip.Items.RemoveAt(5);
            ToolStripItem newMenuItem = new ToolStripMenuItem("Bu punkt hech qanday
vazifa bajarmaydi...");
            menuStrip.Items.Add(newMenuItem);
        }

        #endregion

        public void buildGraph()
        {
            graf.ContextMenuBuilder += new
ZedGraphControl.ContextMenuBuilderEventHandler(Grafik_ContextMenuBuilder);
            GraphPane pane = graf.GraphPane;

            //
            pane.CurveList.Clear();

            Random rnd = new Random();
            //
            //
            string[] nomlar = { "Klssik DH", "Param DH", "ECDH" , "Param ECDH"};//"Param
ECDH"
            double[] yvalues = new double[nomlar.Length];

            #region Tezlikka tekshirish
            //Klassik
            int aa = 443;
            int bb = 567;
            P_ECDH_function();
            Stopwatch st = Stopwatch.StartNew();
            st.Start();
            bosqich1(aa); bosqich2(bb); bosqich3();
            double DH = st.Elapsed.TotalSeconds;

            //Parametrli
            st.Start();
            parambosqich1(aa); parambosqich2(bb); parambosqich3();
            st.Stop();
            double P_DH = st.Elapsed.TotalSeconds;

            //Ellptik ECDH
            st.Start();
            bosqichecdh1(aa); bosqichecdh2(bb); bosqichecdh3();
            st.Stop();
            double ECDH = st.Elapsed.TotalSeconds;

            //Parametrli ECDH

            st.Start();
            bosqichPecdh1(aa); bosqichPecdh2(bb); bosqichPecdh3();
            double P_ECDH = st.Elapsed.TotalSeconds;
```

```
            #endregion
            //double foiz = parametr / klassik;
            yvalues[0] = DH;
            yvalues[1] = P_DH;
            yvalues[2] = ECDH;
            yvalues[3] = P_ECDH;
            //yvalues[3] = 2;
            nomlar[1] = string.Format("{0}({1:0.0})", nomlar[1], P_DH / DH);
            nomlar[2] = string.Format("{0}({1:0.0})", nomlar[2],ECDH / DH);
            nomlar[3] = string.Format("{0}({1:0.0})", nomlar[3], P_ECDH / DH);
            //lblFarqi.Text = string.Format("Klassik al1goritm va Parametrli algoritm
farqi= {0}", foiz);
            pane.YAxis.Title.Text = "Kalitlarni tarqatish algoritmlari";
            pane.XAxis.Title.Text = "Qiyosiy ko'rsatkichlari vaqt hisobida(tezlik
bo'yicha)";
            BarItem curve = pane.AddBar("Diffi- Hellman algoritmining tahlili", yvalues,
null, Color.DodgerBlue);
            Color[] colors = { Color.DarkGreen, Color.Yellow, Color.Red };
            curve.Bar.Fill = new Fill(colors);
            curve.Bar.Fill.Type = FillType.GradientByX;
            curve.Bar.Fill.RangeMin = yvalues.Min();
            curve.Bar.Fill.RangeMax = yvalues.Max();
            //
            pane.YAxis.Type = AxisType.Text;
            //
            pane.YAxis.Scale.TextLabels = nomlar;
            // !
            pane.BarSettings.MinClusterGap = 1.1f;
            pane.XAxis.Scale.MinAuto = true;
            pane.XAxis.Scale.MaxAuto = true;
            // burchak x uqidagi yozuvni
            pane.XAxis.Scale.FontSpec.Angle = 30;

            pane.BarSettings.Base = BarBase.Y;
            //
            pane.XAxis.MajorGrid.IsVisible = true;
            pane.XAxis.MajorGrid.DashOn = 5;
            pane.XAxis.MajorGrid.DashOff = 5;
            //
            pane.YAxis.MajorGrid.IsVisible = true;
            pane.YAxis.MajorGrid.DashOn = 5;
            pane.YAxis.MajorGrid.DashOff = 5;
            //
            pane.YAxis.MinorGrid.IsVisible = true;
            pane.YAxis.MinorGrid.DashOn = 1;
            pane.YAxis.MinorGrid.DashOff = 1;

            pane.XAxis.MinorGrid.IsVisible = true;
            pane.XAxis.MinorGrid.DashOn = 1;
            pane.XAxis.MinorGrid.DashOff = 1;

            pane.Title.Text = "Diffi- Hellman  algoritmining tahlili";
            pane.IsBoundedRanges = true;
            graf.AxisChange();
            graf.Invalidate();
            graf.Refresh();

        }


        #endregion

        private void button42_Click(object sender, EventArgs e)
        {
            bosqichPecdh2(0);
```

```
        }

        private void button34_Click(object sender, EventArgs e)
        {
            bosqichPecdh3();
        }

        private void Form1_Load(object sender, EventArgs e)
        {
            //Yuklanuvchi Logo
            #region Startup Iconni hosil qilish

            Hide();
            bool done = false;
            ThreadPool.QueueUserWorkItem((x) =>
            {
                using (var splashForm = new splashform())
                {
                    splashForm.StartPosition = FormStartPosition.CenterScreen;
                    splashForm.Show();
                    while (!done)
                        Application.DoEvents();
                    splashForm.Close();
                }
            });
            Thread.Sleep(2000);
            done = true;
            Show();
            #endregion
        }

        private void textBox1_TextChanged(object sender, EventArgs e)
        {
            if (!string.IsNullOrEmpty(textBox1.Text))
                button1.Enabled = true;
            else
                button1.Enabled = false;
        }

        private void button49_Click(object sender, EventArgs e)
        {
            if (result.Count > 5)
            {
                int ze = rn.Next(result.Count * 4 / 5, result.Count);
                int dd = result[ze];
                txtP.Text = dd.ToString();
                txtA.Text = rn.Next(dd, 5 * dd).ToString();
                txtB.Text = rn.Next(dd, 5 * dd).ToString();
                bool tek = true;
                int i = 0;
                int b = int.Parse(txtB.Text);
                int p = int.Parse(txtP.Text);
                int a = int.Parse(txtA.Text);
                while (tek)
                {
                    y = System.Math.Sqrt(System.Math.Pow(i, 3) + a * i + b) % p;
                    z = System.Math.Ceiling(y);
                    if (y == z)
                    { txtGX.Text = i.ToString(); txtGY.Text = y.ToString(); tek = false;
}
                    i++;
                }
                txtN.Text = result[result.Count / 2].ToString();
                PniTekshir();
                AniTekshir();
```

```
                BniTekshir();
                richDescription.ForeColor = Color.Green;
                richDescription.Text += string.Format("\r\nG(X,Y)=({0},{1})  Elliptik
egri chiziqqa tegishli bo'lgan nuqta.\r\n\r\n Berilgan oraliqdagi elliptik egri chiziq\n
yechimlari soni N={2} ta\r\n", txtGX.Text, txtGY.Text, txtN.Text);
                qw();
            }
            else
            {
                richDescription.ForeColor = Color.Red;
                richDescription.Text = "Hisoblashlar menyusidan tub sonlar oynasini
tanlang";

            }
        }

    }
}
```