ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Қўлёзма ҳуқуқида
УДК 621.391

Ахмедова Ойдин Пўлатовна

ПАРАМЕТРЛАР АЛГЕБРАСИ АСОСИДА НОСИММЕТРИК КРИПТОТИЗИМЛАР ЯРАТИШ УСУЛИ ВА АЛГОРИТМЛАРИ

Ихтисослик 05.13.19 – «Ахборотлар технологияси, ахборотлар хавфсизлигини таъминлаш тизимлари ва усуллари»

техника фанлари номзоди илмий даражасини олиш учун ёзилган диссертация

А В Т О Р Е Ф Е Р А Т И

Тошкент – 2007

Иш Абу Райҳон Беруний номли Тошкент давлат техника университетида ҳамда Ўзбекистон алоқа ва ахборотлаштириш агентлиги Фан-техника ва маркетинг тадқиқотлари марказининг «Ахборот хавфсизлиги ва криптология» илмий-тадқиқот бўлимида бажарилган.

Илмий раҳбар — техника фанлари номзоди, доцент Назаров Хайриддин Нуритдинович

Расмий оппонентлар — техника фанлари доктори, профессор Каримов Маджит Маликович

техника фанлари номзоди, доцент Рахимжонов Зафар Ёкубович

Етакчи ташкилот — «Ўзбектелеком» акциядорлик компанияси

Ҳимоя Тошкент ахборот технологиялари университети ҳузуридаги Д 001.25.01 ихтисослашган кенгашнинг 2007 йил «31» май соат 10⁰⁰ да ўтадиган мажлисида бўлади.

Манзил: 700084, Тошкент шаҳри, Амир Темур кўчаси, 108, e-mail: tuit.uz.

Диссертация билан Тошкент ахборот технологиялари университетининг кутубхонасида танишиш мумкин.

Автореферат 2007 йил «26» апрел да тарқатилди.

1. ДИССЕРТАЦИЯНИНГ УМУМИЙ ТАВСИФИ

Мавзунинг долзарблиги. Ўзбекистон Республикаси «Телекоммуникациялар тўғрисида» ги қонунида ва Ўзбекистон Республикаси Президентининг 2002 йил 30 майдаги «Компьютерлаштиришни янада ривожлантириш ва ахборот-коммуникация технологияларини жорий этиш тўғрисида» ги Фармонида белгиланган телекоммуникациялар ва маълумотлар узатиш миллий тармоғини ривожлантириш, давлат бошқарувига электрон технологияларни жорий этиш, электрон тижоратни ривожлантириш каби чора-тадбирларнинг амалга оширилиши Ўзбекистон Республикасининг бу соҳада буюк давлатлар қаторидан муносиб ўрин эгаллашида муҳим аҳамият касб этмоқда.

Замонавий ахборот-коммуникация технологиялари пинҳона ва ўта махфий ахборот оқимлари учун қулайликлар яратиш билан бир қаторда янги муаммоларни ҳам ўртага қўймоқда. Ахборот базаларида сақланадиган ва телекоммуникация тизимларида айланаётган ахборот хавфсизлигига таҳдид кескин ошмоқда. Кейинги вақтларда, айниқса, Интернет пайдо бўлгандан бошлаб, ахборот ўғирлаш, ахборот мазмунини эгасидан изнсиз ўзгартириб ва бузиб қўйиш, тармоқ ва серверлардан берухсат фойдаланиш, тармоққа тажовуз қилиш, аввал қўлга киритилган узатмаларни қайта узатиш, хизматдан ёки ахборотга дахлдорликдан бўйин товлаш, жўнатмаларни рухсат этилмаган йўл орқали жўнатиш ҳоллари дунё миқёсида кўпайди. Ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам ***долзарб муаммога айланди.*** Бу муаммони ҳал этиш учун криптологиянинг янги йўналиши бўлган носимметрик криптографияни ривожлантириш зарурияти пайдо бўлди.

Бугунги кунда носимметрик криптография электрон ҳужжат алмашуви, электрон тижорат, электрон савдо, банк тизими фаолияти, солиқ тўловлари тизими ва бошқа соҳаларда илғор ахборот технологияларининг ғоят муҳим асоси бўлиб қолди. Буларга биринчи навбатда электрон рақамли имзо (ЭРИ), махфий шифрлаш калитларини бевосита алмашиш, электрон пул, тармоқ воситаларидан эркин фойдаланишга рухсат бериш криптотизимлари киради.

Кўпгина ривожланган давлатлар ахборот–телекоммуникация тармоқларида махфий ахборотларни хавфсиз узатиш ва электрон рақамли имзо яратишда ўз миллий стандартларидан фойдаланмоқдалар. Алоҳида таъкидлаш лозимки, хорижга экспорт қилинадиган дастурий маҳсулотларда миллий стандартлар қўлланилмайди. Ана шу сабаблар Ўзбекистон Республикасида ҳам носимметрик криптотизимлар алгоритмларини яратиш ва уларни такомиллаштириш муаммоларини ***долзарб қилиб қўйди.***

Илмий-техникавий масаланинг ўрганилганлик даражаси. Криптологияда кенг миқёсда очиқ тадқиқотлар бошланганига эндигина 30 йилдан ошган бўлиб, бу соҳанинг ривожланишига дунёда тан олинган

криптографлар Уитфилд Диффи, Мартин Хеллман, Ральф Меркл, Рон Райвест, Ади Шамир, Леонард Адлеман, Брюс Шнайер, Альфред Менезец, Клаус Шнорр, россиялик ва япониялик бир қанча олимлар ҳамда Ўзбекистонлик Ғ.Ф. Хасанов, М.М. Арипов, М.М. Каримов, Р.И. Исаевлар катта ҳисса қўшмоқдалар. Ўзбекистон Республикасида криптография соҳасида илмий тадқиқотлар бошланганига ҳали кўп (10 йил ҳам) бўлгани йўқ, лекин олим ва мутахассисларимизнинг илмий салоҳияти бардошли миллий криптографик алгоритмлар яратиш учун етарлидир.

Диссертация ишининг илмий-тадқиқот ишлари режалари билан боғлиқлиги. Ушбу диссертация иши Ўзбекистон алоқа ва ахборотлаштириш агентлиги илмий-тадқиқот ишлари режалари доирасида Фан-техника ва маркетинг тадқиқотлари марказининг ахборот хавфсизлиги ва криптология йўналиши бўйича «Маълумотларни шифрлашнинг мураккаб модулли алгоритми ва дастурини ишлаб чиқиш» ва «Ахборотни криптографик муҳофазалаш тизими бардошлилигини баҳолашнинг замонавий усулларини тадқиқ этиш. Криптографик модулларга оид хавфсизлик талабларини ишлаб чиқиш» мавзуларида олиб борилган илмий-тадқиқот ишларига мувофиқ бажарилган.

Тадқиқот мақсади. Мазкур номзодлик ишининг асосий мақсади параметрли алгебрани криптографик масалалар учун параметрлар сонини учтага етказиш йўли билан такомиллаштириб параметрлар алгебрасини яратиш, параметрлар алгебраси асосида носимметрик бардошли криптоалгоритмлар яратиш усули ва бу усулга асосланган бардошли криптоалгоритмлар ишлаб чиқишдир.

Тадқиқот вазифалари. Кўзланган мақсадни амалга ошириш учун диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

а) ҳозирги кунда машҳур бўлган етарли бардошлиликка эга бўлган мавжуд носимметрик криптографик алгоритмларни қиёсий таҳлил этиш;

б) параметрлар алгебрасида носимметрик криптотизимлар яратишга асос бўлган уч параметрли бир томонлама функцияни таклиф этиш ва унинг асосий хоссаларини тадқиқ этиш;

в) параметрлар алгебрасида даража параметрлари учлиги муаммосини шакллантириш ва бу муаммонинг мураккаблигига асосланган криптоалгоритмлар яратиш усулини ишлаб чиқиш;

г) параметрлар алгебраси асосида ЭРИ ва шифрлаш алгоритмларини ишлаб чиқиш.

Тадқиқот объекти ва предмети. Тадқиқот объекти ва предмети сифатида мавжуд носимметрик криптотизимлар яратиш усуллари ва алгоритмлари хизмат қилади.

Тадқиқот усуллари. Диссертация ишида информатика асослари, алгебраик структуралар, носимметрик криптографик тизимлар ва параметрли алгебра усулларидан фойдаланилган.

Ҳимояга олиб чиқилаётган асосий илмий ҳолатлар:

- носимметрик криптотизимларнинг муаммо тури бўйича таснифи;
- параметрлар алгебраси ва унда носимметрик криптографик алгоритмлар яратиш усули, шунингдек, уч параметрли бир томонлама функциялар хоссаларининг тадқиқи;
- параметрлар алгебрасида даража параметрлари учлиги муаммосининг тадқиқи;
- даража параметрлари учлиги муаммосининг мураккаблигига асосланган такомиллаштирилган ЭРИ ва шифрлаш алгоритмлари.

Тадқиқотнинг илмий янгилиги. Тадқиқотнинг илмий янгилиги қуйидагилардан иборат:

а) параметрлар алгебраси ва унда носимметрик криптографик алгоритмлар яратиш усули ишлаб чиқилиши;

б) носимметрик криптотизимларнинг бардошлилигини уч параметрли яширин йўлли бир томонлама функция асосида ошириш усули таклиф этилиши;

в) параметрлар алгебрасида даража параметрлари учлиги муаммоси мавжудлигининг аниқланиши ва асосланиши;

г) бардошлилиги даража параметрлари учлиги муаммосининг мураккаблигига асосланган такомиллаштирилган ЭРИ ва шифрлаш алгоритмлари.

Тадқиқот натижаларининг илмий ва амалий аҳамияти.

1. Параметрлар алгебрасида носимметрик криптографик алгоритмлар яратиш усули асосида ишлаб чиқилган криптоалгоритмлар республикамизнинг ахборот ва коммуникация тизимларида қўллаш учун мавжуд криптотизимларга нисбатан бардошлилиги юқори бўлган криптотизимлар ишлаб чиқишда қўлланилиши мумкинлиги билан аҳамиятлидир.

2. Даража параметрлари учлиги асосида ишлаб чиқилган криптоалгоритмлардан ахборотнинг криптографик муҳофазаси бўйича миллий стандартлар ишлаб чиқишда фойдаланиш мумкин.

3. Диссертация натижалари ўқув муассасаларида ахборот хавфсизлиги бўйича кадрлар тайёрлашда криптография фанидан таълим бериш жараёнида қўлланилиши мумкинлиги билан аҳамиятли.

Тадқиқот натижаларининг жорий қилиниши. Тадқиқот иши натижаларидан ахборотнинг криптографик муҳофазаси бўйича O'z DSt 1092:2005 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари» ва O'z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар» Ўзбекистон давлат стандартларини ишлаб чиқишда, Фан-техника ва маркетинг тадқиқотлари маркази қошидаги электрон рақамли имзо калитларини рўйхатга олиш марказининг муҳофазаланган электрон почта Е-ХАТ тизимида ЭРИ

шакллантириш жараёнида, Ўзбекистон алоқа ва ахборотлаштириш агентлиги Фан-техника ва маркетинг тадқиқотлари марказининг ахборот хавфсизлиги ва криптология йўналиши бўйича олиб борилган илмий-тадқиқот ишлари бўйича илмий ҳисоботлар асосида ишлаб чиқилган давлат стандартлари ҳамда меъёрий ҳужжатларда фойдаланилган.

Тадқиқотнинг апробациядан ўтганлиги. Диссертация ишининг асосий мазмуни ва натижалари «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги» республика семинарида (Тошкент ш. 3 декабрь 2003 й.), «Алоқа ва ахборот технологияларининг ҳозирги ҳолати ва ривожланиш истиқболлари» халқаро илмий-техник конференциясида (Тошкент ш. 11-12 май 2005 й.), «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги» республика семинарида (Тошкент ш. 24 ноябрь 2005 й.), «Актуальные проблемы использования электронной цифровой подписи» халқаро илмий-амалий конференциясида (Тошкент ш. 24-25 май 2006 й.), «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал этиш йўллари» республика семинарида (Тошкент ш. 18 октябрь 2006 й.) ва Тошкент давлат техника университетининг «Электроника ва автоматика» факультети илмий семинарида (Тошкент ш. 23 декабрь 2006 й.) ва ЎзААА ФТМТМ илмий-техник семинарида (Тошкент ш. 2 март 2007 й.) маъруза қилинган ва муҳокамадан ўтган.

Натижаларнинг эълон қилинганлиги. Диссертациянинг асосий моҳияти ва мазмуни 16 та илмий ишларда акс этган. Шулардан 9 таси журнал мақолалари, қолганлари илмий тўпламларда чоп этилган, 1 таси CD-дискда тарқатилган. «Рақамли имзо шакллантириш ва аутентификациялаш усули» номли ихтиро учун Ўзбекистон Давлат патент идораси томонидан IAP 030770-сон патенти берилган.

Диссертация ишининг тузилиши ва ҳажми. Диссертация иши кириш қисми, 4 та бўлим, хулоса, 151 та номдаги фойдаланилган адабиётлар рўйхати ва 9 та иловадан иборат. Диссертация ишининг асосий қисми 125 варақ машина матнида ёритиб берилган.

2. ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

Кириш қисмида диссертация иши мавзусининг долзарблиги, илмий-техникавий масаланинг ўрганилганлик даражаси, тадқиқот объекти ва предмети, шунингдек, тадқиқотнинг мақсади ва вазифалари аниқланиб асослаб берилди. Илмий ишни бажаришда фойдаланилган тадқиқот усуллари, тадқиқотнинг илмий янгилиги, тадқиқот натижаларининг илмий ва амалий аҳамияти, ҳимояга олиб чиқилаётган асосий илмий ҳолатлар, тадқиқотнинг апробациядан ўтганлиги, натижаларнинг эълон қилинганлиги, диссертация ишининг тузилиши ва ҳажми тўғрисидаги ахборотлар баён этилган.

Биринчи бўлимда криптография соҳасидаги етакчи давлатлар АҚШ, Россия, Европа мамлакатлари ва Японияда ошкора криптография соҳасида энг кўп қўлланиладиган, энг ишончли деб тан олинган криптографик тизимларнинг қиёсий таҳлили ва таснифи келтирилган.

Ушбу номзодлик диссертация ишида мавжуд носимметрик криптотизимлар уларнинг бардошлилигини таъминлашга асос бўлган мураккаб муаммо тури бўйича қуйидагича таснифланади (1-жадвал).

1-жадвал

Муаммо тури бўйича носимметрик криптотизимлар таснифи

Муаммолар	Муаммолар таърифи	Криптотизимлар
Факторлаш муаммоси	Бутун мусбат сон **n** берилган бўлса, унинг туб факторлари топилсин: яъни, $n=p_1^{e1}p_2^{e2}...p_k^{ek}$ кўринишда ифодалансин, бу ерда p_i турли туб сонлар, e_i - бирдан кам бўлмаган даража кўрсаткичлари.	RSA (k=2) ESIGN, OSS А.Фиат ва А.Шамир, PGP, RPK
Дискрет логарифм муаммоси	Туб сон **p** учун, чекли майдон Z_{p^*} да ҳосил қилувчи (генератор) элемент α ҳамда $\beta \in Z_{p^*}$ берилган бўлса, шундай $0 \le x \le p-2$ бўлган бутун **x** сон топилсинки, унда $\alpha^x \equiv \beta \pmod p$ бўлсин, бу ерда **x** – даража кўрсаткичи.	Эл Гамал, Шнорр, DSA, ГОСТ Р 34.10-94
Эллиптик эгри чизиқли дискрет логарифм муаммоси	F_q чекли майдонда эллиптик эгри чизиқ **E**, **P**, $Q \in E(F_q)$ берилган бўлса, **Q=dP** шартни қаноатлантирувчи **0** ва **n-1** оралиғида мавжуд бўлган **d** сони топилсин. Бу ерда барча ҳисоблашлар **q** модули бўйича бажарилади ва a^3+b^2 қиймати 0 дан фарқли; **q** нинг қиймати 3 дан катта туб сон; **n – P** нуқтасининг тартиби (**nP = 0**, **0 - E(F_q)** нинг эллиптик эгри чизиқ нуқталари устида қўшиш амалига нисбатан бирлик элементи).	ГОСТ Р 34.10-2001, ECDSA, ДСТУ 4145-2002
Бошқа муаммолар: Даража параметри муаммоси	Туб сон **p** учун, параметри **R** бўлган чекли майдон $Z(R)_{p^*}$ да $\beta \in Z(R)_{p^*}$ берилган бўлиб, $\beta \equiv \alpha^{\backslash x} \pmod p$ бўлса, ҳосил қилувчи элемент α, параметр **R** ва **x** топилсин. Бу ерда $\backslash$ - параметр **R** билан **p** модул бўйича даражага ошириш рамзи.	O'z DSt 1092:2005

1-жадвалда келтирилган тасниф бўйича факторлаштириш муаммосининг мураккаблигига асосланган RSA, ESIGN, Он, Шнорр ва Шамир (OSS), Амос Фиат ва Ади Шамир, PGP, RPK ва бошқа криптотизимларнинг ўзига хос томонлари баён этилди. Булар орасида ҳозирги кунда амалиётда энг кўп қўлланиладиган криптотизим RSA ҳисобланади. У кўпгина хорижий стандартларга, шу жумладан, ISO 9796, SWIFT, Австралия стандарти AS2805.6.5.3, ANSI X9.31 DSA ва X9.44 ларга асос қилиб олинган.

Эл Гамал, Шнорр, DSA ва ГОСТ Р 34.10-94 рақамли имзолари бир-бирига жуда ўхшаш схемалар ҳисобланади. Улар моҳияти ва бардошлилиги жиҳатидан дискрет логарифм муаммосининг мураккаблигига асосланган умумий рақамли имзолар схемасининг ҳар хил намуналаридир. Эл Гамал, DSA ва ГОСТ Р 34.10-94 алгоритмларида ЭРИни шакллантириш жараёнида тескарилаш амали ишлатилиши сабабли паст эффективликка эга.

Бардошлилиги эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган Россиянинг ГОСТ Р 34.10 – 2001 ва АҚШнинг ECDSA ЭРИ криптотизимларида узунлиги жуда қисқа бўлган калитлардан фойдаланилади, шу туфайли уларда RSA алгоритмига кўра калитлар **100** марта тезроқ ҳосил қилинади ва анча кам жой эгаллайди. Масалан, **97** битли калитга эга бўлган шифрматнни бузишга уриниш **512** битли калитга эга бўлган RSA носимметрик шифрини бузишдан кўра икки марта қийинроқдир. Эллиптик эгри чизиққа асосланган ЭРИ алгоритмларида калит ўлчамини ошириш билан имзо яратиш сезиларли даражада тезроқ амалга оширилади, имзони текшириш эса анча секинроқ кечади.

Шуни айтиб ўтиш керакки, криптографик алгоритмларнинг криптотаҳлилларга бардошлилиги криптотизимни амалиётга тадбиқ қилишда томонларнинг келишиб олинган тартиб-қоидалари мажмуи – криптотизим протоколига ҳам жуда боғлиқ бўлади.

Юқорида келтирилган криптотизимларнинг асосий камчиликларидан бири, бузғунчи криптотизим асосига олинган муаммони етарлича аниқ кўя олганда ва унинг бу муаммони ҳал қилишга ресурслари етарлича бўлганда, қабул қилувчига келиб тушган рақамли имзо сохта бўлса, имзоловчи шахсда имзонинг сохталигини исботловчи далиллар ва маълумотларнинг йўқлигидир.

1-жадвалда келтирилган таснифга биноан криптотизимларнинг бардошлилигини таъминлашга асос бўлган яна бир бошқа муаммо – даража параметри муаммосидир. Бу муаммо турига Ўзбекистон миллий стандарти O'z DSt 1092:2005 киради. Уни яратишда мавжуд алгоритмларга хос камчиликларни бартараф этишга эътибор берилди. Шу мақсадда криптография соҳасидаги Ўзбекистон Республикасининг дастлабки давлат стандарти O'z DSt 1092:2005 ни яратиш учун математик асос сифатида П.Ф. Хасанов ва Х.П. Хасанов томонидан таклиф этилган параметрли алгебра қабул қилинган. Унда модул арифметикасининг яширин йўлли янги

бир томонлама функцияси қўлланилади, бунда ҳисоблашлар қийинлик даражаси бўйича даражага кўтариш амаллари каби енгил амалга оширилади, функцияни тескарилаш эса дискрет логарифм муаммосини ечиш жараёнидагидан кам бўлмаган ҳисоблаш сарфлари ва вақт талаб қилади. Анъанавий бир томонлама даражага кўтариш функцияси битта яширин йўлга эга бўлиб, ушбу бир томонлама функциянинг хусусий ҳолидир. Унда яширин йўллар сонининг учта бўлиши мумкинлиги бардошлиликни ошириш учун қўшимча имкониятлар яратади.

O'z DSt 1092:2005 да ЭРИни шакллантириш жараёнига ЭРИнинг ҳақиқийлигини тасдиқлаш жараёнида қўлланиладиган сеанс калити тартиботини киритиш ЭРИ сохталигини аниқлашга хизмат қилади. Мазкур стандартда ***даража асосининг махфийлиги гояси муаллифга тегишлидир.*** O'z DSt 1092:2005 да даража асосининг махфий бўлиши эвазига унинг бардошлилиги DSA и ГОСТ Р 34.10-94 ларнинг бардошлилигидан икки марта катта бўлади.

Параметрли алгебрадан фойдаланиш нафақат O'z DSt 1092:2005 стандартини, балки кўпгина мавжуд ошкора калитли ЭРИ алгоритмларини ҳам такомиллаштиришнинг янги йўналишини очиб беради.

Иккинчи бўлимда ***муаллиф ва Х.П. Хасанов ҳаммуаллифлигида*** параметрлар сонини учтага етказиш йўли билан параметрли алгебрани такомиллаштирилиб ҳосил қилинган ***параметрлар алгебраси*** баён этилган. Шунингдек, унда уч параметрли яширин йўлли бир томонлама функциялар ва уларнинг хоссалари, ўзаро мос бир қийматли алмаштириш ифодалари ва даража параметрлари учлиги муаммоси келтирилган.

Агар модул арифметикасида параметр **R** билан бир қаторда яна иккита, яъни **a** ва **b** параметрлардан фойдаланилса, параметрлар учлиги **<a, b, R>** билан кўпайтириш амали ҳосил бўлади ва уни қуйидаги кўринишда ифодалаш мумкин:

$$x \circledR_3 y \equiv a*x + y*(b+R*x) \pmod{n}. \qquad (1)$$

Бу ерда

$n \in \{p, p_1*p_2\}$ модул, p – туб сон, p_1, p_2 – ҳар хил туб сонлар,

$\circledR_3$ – параметрлар учлиги **<a, b, R>** билан кўпайтириш амали рамзи, $a \geq 1$, $b \geq 1$, $R \geq 0$.

Параметрлар учлиги **<a, b, R>** билан кўпайтириш амалига доир мисол қуйидаги 2-жадвалда келтирилган.

2-жадвал

Параметрлар учлиги <a, b, R> билан кўпайтириш

n	a	b	R	x	y	a*x	b+R*x	y*(b+R*x)	x ®₃ y
23	3	7	19	16	7	2	12	15	17
107	3	7	19	16	15	48	97	64	5

Параметрлар учлиги <a, b, R> билан кўпайтириш амали берилган бутун сонлар чекли тўпламида ***бирлик элементи*** 0 га тенг.

(b+R*x) (mod n) сони модул **n** билан ўзаро туб бўлганда тўплам элементи **x** учун тескари ***ўнг элемент*** x^{III-1} ***мавжуд.***

Тескари ўнг элемент x^{III-1} қуйидагича ҳисобланади:

$$x^{III-1} \equiv -a*x*(b+R*x)^{-1} \pmod n, \qquad (2)$$

бу ерда $^{-1}$ – **n** модул бўйича тескарилаш амали рамзи.

Уч параметрли тескари ўнг элемент учун

$$x \circledR_3 x^{III-1} \equiv 0 \pmod n \qquad (3)$$

инверсия аксиомаси қаноатлантирилади.

Қуйидаги 3-жадвалда мазкур аксиома кучга эга эканлигига доир мисол **n=257** модул учун акс этган.

Мазкур жадвалда тескари ўнг ва чап элемент аксиомаси фақат **a=1, b=1, R≥0** бўлганда қаноатлантирилиши ўз ифодасини топган.

3-жадвал

Тескари ўнг элемент учун инверсия аксиомаси қаноатлантирилиши

a	b	R	x	x^{III-1}	$x \circledR_3 x^{III-1}$	$x^{III-1} \circledR_3 x$
19	27	45	23	161	0	181
3	1	45	23	152	0	1
5	7	1	23	39	0	225
1	5	45	23	148	0	14
1	1	1	23	74	0	0
1	1	45	23	222	0	0

Айният аксиомаси фақат параметр **a=1** бўлгандагина қаноатлантирилади:

$$x \circledR_3 0 \equiv x. \qquad (4)$$

Бироқ, параметр **a > 1** учун

$$x \circledR_3 0 \equiv a*x \pmod n,$$

$$(x \circledR_3 0) \circledR_3 0 \equiv a^2*x \pmod n,$$

:

$$(..((x \circledR_3 0) \circledR_3 0)... \circledR_3 0) \equiv a^m *x \pmod n \qquad (5)$$

таққосламалар тизими ўринлидир. Бу ерда **m** – параметрлар учлиги билан бирлик элементига кўпайтиришлар сони.

Юқорида келтирилган амаллар асосида шаклланган алгебра қуйидагича таърифланади.

Таъриф. F_n – чекли, яъни, **n** та элементдан иборат бутун сонлар тўплами, шу тўпламда берилган параметрлар **a, b, R** бўлса, $\circledR_3$ – F_n устида

аниқланган параметрлар учлиги <a, b, R> билан кўпайтириш амали бўлса, $(F_n; ®_3)$ - жуфтлик ***параметрлар алгебраси*** деб аталади.

Параметрлар учлиги <a, b, R> билан кўпайтириш амали уччала параметр 1 дан катта натурал сон бўлса, ассоциативлик ва коммутативлик аксиомаларини қаноатлантирмайди, бинобарин R - натурал сон бўлганда параметрлар учлиги алгебраси мультипликатив группа эмас, фақат R=0 бўлгандагина аддитив группанинг барча аксиомалари қаноатлантирилади.

Параметрлар алгебраси a=1, b=1 ва R>0 бўлганда мултипликатив ***коммутатив группа аксиомаларини қаноатлантиришини*** эътиборга олган ҳолда криптотизимлар яратишда бир томонлама функцияларни ҳосил қилишда дастлаб a=1, b=1 ва R≥1 параметрлардан фойдаланиб, сўнгра бардошлиликни янада ошириш мақсадида махфий параметрлар сифатида a>1 ёки b>1 ёки a=b>1 олиш мақсадга мувофиқдир.

Таъриф. Модул арифметикасида параметрлар алгебрасида параметрлар учлиги <a, b, R> билан даражага ошириш функцияси ***уч параметрли бир томонлама функция*** (қисқача, уч параметрли функция) деб аталади.

Мазкур диссертация ишида асосан 2 хил модул $n \in \{p, p_1*p_2\}$ бўйича аниқланган уч параметрли функцияларга эътибор қаратилган. Модул n бўйича асос x ни параметрлар учлиги <a, b, R> билан e даражага ошириш натижаси $x^{\langle\langle\langle e} \pmod n$ шаклида ифодаланган, бу ерда $e \in \{0,1,...\varphi(n)\}$, $\varphi(n)$ – Эйлер пи - функцияси, $\langle\langle\langle$ – <a, b, R> параметрлар учлиги билан даражага ошириш рамзидир.

Мазкур диссертация ишида уч параметрли бир томонлама функцияларнинг хоссалари келтирилган бўлиб, бу хоссалар функция қийматини исталган даража кўрсаткичи учун ҳисоблаш учун етарлидир.

Келтирилган уч параметрли функция хоссаларининг бир параметрли диаалмаштиришлар функцияси хоссаларидан фарқли томонлари криптография ва криптотаҳлил масалаларига янгича ёндашувларни тақозо этади ҳамда криптология муаммоларини мураккаблаштиради. Бундай муаммолар қаторига мавжуд муаммолардан тамойили бўйича фарқ этган даража параметрлари учлиги муаммоси ҳамда унга мос бўлган дискрет логарифм муаммоси ва Диффи-Хеллман муаммоси киради.

Уч параметрли функциялар асосида амалий криптотизимлар яратиш юқори кўрсаткичли бир томонлама функциялардан фойдаланишга асосланади. Уч параметрли функцияни ҳисоблаш бир параметрли диаалмаштиришлар функциясини ҳисоблаш ва уни унга мос уч параметрли функция билан алмаштириш асосида амалга оширилади. Бунда бошланғич параметрлар учлиги $<a_1, b_1, R_1>$ билан берилган уч параметрли функцияни натижавий параметрлар учлиги $<a_2, b_2, R_2>$ билан берилган уч параметрли функцияга ўзаро мос бир қийматли алмаштириш ифодаларидан фойдаланилади. Бундай ўзаро мос бир қийматли алмаштириш ифодалари илмий ишда келтирилган.

Носимметрик алгоритмларни амалга ошириш жараёнларида анъанавий алгебранинг кўпайтириш, айириш ва тескарилаш амаллари қаторида бутун сонлар устида берилган параметрлар учлиги <a, b, R> билан кўпайтириш, сонни квадратга ошириш, сонни берилган даража кўрсаткичига ошириш ва соннинг тескари қийматини топиш амаллари қўлланилади.

Мазкур диссертация ишида ишлаб чиқилган криптотизимларнинг бардошлилиги уч параметрли функцияда қатнашадиган параметрлар учлиги <a, b, R> нинг муштарийлар жуфтидан бошқа кимсалар учун махфийлигига асосланган. Криптография бўйича очиқ адабиётда бундай муаммо келтирилмаган.

Даража параметрлари учлиги муаммоси қуйидагича таърифланади:

Таъриф. **GF(n)** чекли майдоннинг ҳосил қилувчи элементи **x**, параметрлар учлиги **<a, b, R>** билан уч параметрли функция қиймати $Y \equiv x^{\langle\langle e \rangle\rangle} \pmod n$ берилган бўлса, даража кўрсаткичи **e** ва параметрлар учлиги **<a, b, R>** топилсин, бу ерда $n \in \{p, p_1 * p_2\}$.

Катта қийматга эга бўлган туб ва мураккаб модуллар учун **a>1, b>1, R>1** бўлган даража параметрлари учлиги муаммосини эффектив ҳал этиш йўллари муаллифга маълум эмас.

<u>**Учинчи бўлимда**</u> параметрли алгебрада яратилган носимметрик криптотизимлардан параметрлар учлиги алгебрасидан фойдаланган ҳолда ***носимметрик криптотизим яратиш усули*** келтирилган. Унда параметрлар алгебрасида носимметрик криптотизим яратиш усули таърифи, параметрли алгебрада ва параметрлар алгебрасида К. Шнорр электрон рақамли имзо схемасининг аналоглари, параметрли алгебрада Полиг-Хеллман шифри прототип сифатида танланган ҳол учун яратилган криптотизим, параметрлар алгебраси асосида криптотизим яратишга RSA усулида ёндашувлар баён этилган.

Мазкур диссертация ишида ишлаб чиқилган параметрли алгебрада яратилган носимметрик криптотизимлардан параметрлар учлиги алгебрасидан фойдаланган ҳолда носимметрик криптотизим яратиш усули қуйидагича таърифланади.

Таъриф. Бошланғич криптотизим-прототип танлаш ва унда фойдаланилган параметр ва функцияларни, шу жумладан параметр **R>0** билан кўпайтириш амали асосида амалга ошириладиган даража **e** га ошириш (^{e}) функциясини параметрлар учлиги **<a, b, R>** билан даража **e** га ошириш ($^{\langle\langle e \rangle\rangle}$) функцияси билан ўзаро бир қийматли алмаштириш ифодалари асосида алмаштириш натижасида криптотизим яратиш усули ***параметрлар учлиги алгебрасида носимметрик криптотизим яратиш усули*** деб аталади.

Агар параметрли алгебрада бошланғич прототипга мос носимметрик криптотизим бўлса, унда уни криптотизим-прототип сифатида қабул қилинади, акс ҳолда криптотизим-прототип яратилади.

Ўз навбатида мазкур усул криптотизим-прототип сифатида қабул қилиш ҳолида параметрли алгебрада ўрнатилган носимметрик криптотизим параметрлари ва амаллари сатри

a=1	b=1	R>0	®	\-1	\e

ўрнига ўзаро бир қийматли алмаштириш ифодалари асосида мос тарзда параметрлар учлиги алгебрасида параметрлар ва амаллари сатри

a>1	b>1	R>0	$®_3$	\\\-1	\\\e

билан алмаштиришдан иборат.

Бу ерда

\-1 – параметр R билан тескарилаш амали рамзи,

\e – параметр R билан даражага ошириш рамзи,

\\\-1 – параметрлар учлиги <a, b, R> билан тескарилаш амали рамзи,

\\\e – параметрлар учлиги <a, b, R> билан даражага ошириш рамзи.

Бунда криптотизим параметрлари тўпламига қўшимча тарзда a>1 ёки b>1, ёки a>1 ҳамда b>1 параметр киритилади.

Параметрлар учлиги <a, b, R> ошкора (очиқ) бўлганда мавжуд носимметрик криптотизимлар билан тенг бардошлиликка эга бўлган криптотизим ҳосил бўлади, параметрлар учлиги <a, b, R> махфий бўлганда мавжуд носимметрик криптотизимларга нисбатан юқори бардошлиликка эга бўлган криптотизимлар ҳосил бўлади.

Мазкур диссертация ишида бир томонлама уч параметрли функциядан фойдаланиб мавжуд носимметрик криптотизимларни такомиллаштириш масалаларини амалга ошириш мумкинлиги Шнорр, Полиг-Хэллман ва RSA усуллари бўйича ишлаб чиқилган такомиллашган криптоалгоритмларда кўрсатиб берилди.

Диссертация ишида параметрлар алгебраси асосида криптотизим яратишга RSA усулида ёндашувлар асосида ишлаб чиқилган схема мавжуд RSA криптотизимидан фарқли ўлароқ, маълумотларни хэшлаш тартиботидан ҳоли бўлишига ва унга оид шифрлашнинг коммутативлиги билан алоқадор камчиликларни бартараф этишга имкон беради ва қонуний фойдаланувчилар учун ўзининг RSA криптотизими билан тенг бардошлилиги билан, қонуний фойдаланувчи бўлмаганлар учун эса RSA криптотизимига нисбатан юқори бардошлилиги билан характерланади. Ишлаб чиқилган криптотизимларнинг бардошлилиги махфий параметрлар учлиги ҳисобига мавжуд криптотизимларга нисбатан юқори бўлиши ва янги протоколлар ишлаб чиқиш имконияти туғилганлиги кўрсатиб берилди.

Тўртинчи бўлимда ***уч параметрли бир томонлама функциялар асосида такомиллаштирилган*** Шнорр, Полиг-Хэллман ва RSA алгоритмларига аналог бўлган алгоритмлар ва уларнинг блок-схемалари келтирилган.

Қуйида, мисол тариқасида, параметрлар алгебрасида Шнорр ЭРИ алгоритмининг аналогини келтириш билан чекланамиз.

M хабар остига қўйиладиган электрон рақамли имзо **(e, y)** ни шакллантириш алгоритми қуйидагича берилади.

Кириш: хабар **M** ЭРИнинг махфий калити **(s, u, g)**, томонлар жуфти аро биргаликдаги махфий калит R_{ij}, модул **p** ва **q** сони.

Чиқиш: ЭРИ **(e, y)**.

1-қадам. Параметрлар учлиги $<1, 1, R_{ij}>$ дан фойдаланиб

$x \equiv (R_{ij}^{-1} * g)^{\backslash\backslash r} \pmod p$ ни ҳисобланг.

2-қадам. $M \circledast_{ij} x \equiv M + x*(1+R_{ij}*M) \pmod p$ ни ҳисобланг.

3-қадам. $e = H(M \circledast_{ij} x)$ ни ҳисобланг.

4-қадам. $y \equiv u^{-1}*(r - s*e) \pmod q$ ни ҳисобланг ва **(e, y)** ни чиқишга беринг ҳамда ҳисоблашни тўхтатинг.

M хабар остига қўйилган электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш алгоритми қуйидагича берилади.

Кириш: хабар **M'**, ЭРИнинг ошкора калитлари учлиги $(\nu_{1abR}, \nu_{2abR}, g_{ab1})$, модул **p** ва **q** сони, ЭРИ **(e, y)**, томонлар жуфти аро биргаликдаги махфий калитлар **(a, b, R_{ij})**.

Чиқиш: «имзо ҳақиқий» ёки «имзо ҳақиқий эмас».

1-қадам.

$\nu_1 \equiv (g_{ab1}+b-1)*(\nu_{1ab1}*(g_{ab1}+b)+(a-1)*g_{ab1})*(g_{ab1}*(g_{ab1}+b-1+a))^{-1} \pmod p$ ни ҳисобланг.

2-қадам.

$\nu_2 \equiv (g_{ab1}+ b-1)*(\nu_{2ab1}*(g_{ab1}+ b)+(a-1)*g_{ab1})*(g_{ab1}*(g_{ab1}+ b-1+a))^{-1} \pmod p$ ни ҳисобланг.

3-қадам. $x' \equiv (R_{ij}^{-1}*\nu_2)^{\backslash\backslash y} \circledast (R_{ij}^{-1}*\nu_1)^{\backslash\backslash e} \pmod p$ ни ҳисобланг.

4-қадам. $M' \circledast_{ij} x' \equiv M' + x'*(1+ R_{ij} *M') \pmod p$ ни ҳисобланг.

5-қадам. $e' = H(M' \circledast_{ij} x')$ ни ҳисобланг.

6-қадам. Агар $e = e'$ бўлса, унда чиқишга «имзо ҳақиқий»ни беринг, агар $e \neq e'$ бўлса, унда «имзо ҳақиқий эмас» ни қабул қилинг.

Таклиф этилаётган усул билан электрон рақамли имзо яратиш сеанс калитисиз ёки сеанс калитили маромда амалга оширилиши мумкин.

Қуйидаги 4- ва 5-жадвалларда параметрлар учлиги билан Шнорр ЭРИ алгоритмининг аналоги бўйича ЭРИ шакллантириш ва унинг ҳақиқийлигини тасдиқлашга доир мисоллар келтирилган.

4-жадвал

ЭРИ шакллантириш

p	q	s	h	g	u	u^{-1}	a	b	R_{ij}	R_{ij}^{-1}	ν_1	ν_2
107	53	30	3	15	13	49	3	5	29	48	32	52
107	53	30	3	15	13	49	5	7	31	38	32	52

4-жадвалнинг давоми

v_{1ab1}	v_{2ab1}	g_{ab1}	r	x	M	$M®_{ij}x$	$e=H(M®_{ij}x)$	y
17	87	11	19	73	8	4	4	27
102	10	9	19	89	15	80	80	23

5-жадвал

ЭРИ ҳақиқийлигини тасдиқлаш

p	q	a	b	R_{ij}	R_{ij}^{-1}	g_{ab1}	M'	$e=H(M®_{ij}x)$	y	v_{1ab1}	v_{2ab1}
107	53	3	5	29	48	11	8	4	27	17	87
107	53	5	7	31	48	9	15	80	23	102	10

v_1	v_2	$(R_{ij}^{-1}*v_2)^{\|y}$	$(R_{ij}^{-1}*v_1)^{\|e}$	x'	$M'®_{ij}x'$	$e'=H(M'®_{ij}x')$
32	52	54	53	73	4	4
32	52	77	57	89	80	80

Параметрлар алгебраси асосида ишлаб чиқилган Шнорр, Полиг-Хэллман ва RSA алгоритмларига аналог бўлган алгоритмлар мавжуд криптотизимларга нисбатан ***параметрлар учлиги ҳисобига юқори бардошлиликка эга бўлиши*** билан характерланади.

3. ХУЛОСА

1 Мазкур диссертация ишида криптография соҳасидаги етакчи давлатлар АҚШ, Россия, Европа мамлакатлари ва Японияда ошкора криптография соҳасида энг кўп қўлланиладиган, энг ишончли деб тан олинган криптотизимларнинг ўзига хос томонлари таҳлил этилди ва улар бардошлилигини таъминлашга асос бўлган муаммолар таснифланди. Мавжуд носимметрик криптотизимларнинг кўпчилиги модуллар арифметикасида яширин йўлли бир томонлама осон ҳисобланадиган функцияларга асосланади ва уларнинг бардошлилиги эса дискрет логарифм, факторлаш, эллиптик эгри чизиқли дискрет логарифм ва даража параметри муаммоларидан бирининг мураккаблигига асосланади.

2 Мавжуд носимметрик криптографик алгоритмларни қиёсий таҳлил қилиш натижасида параметрли алгебра асосида яратилган Ўзбекистон Республикасининг дастлабки давлат стандарти O'z DSt 1092:2005 да ЭРИни шакллантириш ва унинг ҳақиқийлигини тасдиқлашда махфий параметрли алгебрадан, ошкора сеанс калитидан ҳамда муаллиф томонидан таклиф этилган махфий даража асосидан фойдаланиш каби ЭРИ алгоритмининг бардошлилигини оширишга йўналтирилган ўзига хос томонлар кўрсатиб берилди. Бу ўз навбатида параметрли алгебрадан фойдаланиш кўпгина мавжуд ошкора калитли ЭРИ алгоритмларини такомиллаштиришнинг янги йўналишини очиб беришини кўрсатади.

3 Параметрли алгебра криптографик масалалар учун параметрлар сонини учтага етказиш йўли билан параметрлар алгебраси кўринишида такомиллаштирилди. Модул арифметикасида параметр **R** билан бир қаторда яна иккита, яъни **a** ва **b** параметрлардан фойдаланиш параметрлар учлиги **<a, b, R>** билан кўпайтириш амалини аниқлайди. Мазкур кўпайтириш амали асосида яширин йўллари уч ва ундан ортиқ бўлган бир томонлама функция таклиф этилди.

4 Параметрлар алгебрасининг хоссалари ва унинг асосида носимметрик криптотизимлар яратишга асос бўлган уч параметрли бир томонлама функциянинг асосий хоссалари тадқиқ этилди. Уч параметрли бир томонлама функцияларни ўзаро мос бир қийматли алмаштириш ифодалари ишлаб чиқилди. Криптографик алгоритмлар ишлаб чиқиш учун даража параметрлари учлиги муаммоси мавжудлиги аниқланди ва таърифланди.

5 Параметрлар алгебрасида даража параметрлари учлиги муаммосининг мураккаблигига асосланган носимметрик криптоалгоритмлар яратиш усули ишлаб чиқилди. Бошланғич криптотизим-прототип танлаш ва унда фойдаланилган параметр ва функцияларни, шу жумладан параметр **R>0** билан кўпайтириш амали асосида амалга ошириладиган даража **e** га ошириш (^{e}) функциясини параметрлар учлиги **<a, b, R>** билан даража **e** га ошириш ($^{\langle e \rangle}$) функцияси билан ўзаро бир қийматли алмаштириш ифодалари асосида алмаштириш натижасида криптотизим яратиш усули ***параметрлар учлиги***

алгебрасида носимметрик криптотизим яратиш усули деб аталади. Мазкур усул нафақат мавжуд носимметрик криптотизимларни улардан кам бўлмаган бардошлиликка эга бўлган уларга ўхшаш криптотизимлар яратиш билан такомиллаштириш имкониятини, балки махфий параметрлардан турлича фойдаланиш асосида мавжуд криптотизимларга нисбатан юқори бардошлиликка эга бўлган криптотизимлар яратиш имкониятини ҳам беради.

6 Бир томонлама уч параметрли функциядан фойдаланиб мавжуд носимметрик криптотизимларни такомиллаштириш масалаларини амалга ошириш мумкинлиги RSA, Шнорр ва Полиг-Хэллман алгоритмларига аналог бўлган такомиллашган криптоалгоритмларда кўрсатиб берилди. Такомиллаштириш натижасида уларнинг бардошлилиги махфий параметрлар учлиги ҳисобига кескин ошади ва янги протоколлар ишлаб чиқиш имконияти пайдо бўлади.

7 Ишлаб чиқилган криптоалгоритмлар ва параметрлар алгебраси республикамизнинг ахборот ва коммуникация тизимларида қўллаш учун янги носимметрик криптотизимлар ишлаб чиқишда, криптография йўналишида илмий тадқиқотлар олиб боришда ҳамда ўқув муассаларида криптография фанидан таълим беришда қўлланилиши мумкин.

4. ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ

1. Хасанов П.Ф., Хасанов Х.П., Хасанов С.П., Хасанов З.П., Хасанов Ш.П., Ахмедова О.П.. Рақамли имзо шакллантириш ва аутентификациялаш усули // Ўзбекистон Давлат патент идораси томонидан берилган IAP 03070-сон патенти. Устуворлик санаси: 2002.14.08.

2. Исаев Р.И., Хасанов П.Ф., Назарова М.Х. Ахмедова О.П. Диаэкспоненциальный алгоритм шифрования данных // Информационная безопасность в сфере связи и информатизации: Материалы республиканского семинара 3 декабря 2003. – Ташкент. – С. 38-39.

3. Ахмедова О.П. Электрон рақамли имзо учун мавжуд очиқ калитли криптотизимларнинг қиёсий таҳлили // InfoCOM.UZ. – Тошкент, 2005, №7. – 36-40 бетлар.

4. Ахмедова О.П. Криптология ва криптографик тизимлар // Информационная безопасность в сфере связи и информатизации: Тезисы докл. респ. сем. 24 ноября 2005. – Ташкент. – С. 74-77.

5. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Мазгаров Б.А., Ахмедова О.П. О проектах государственного стандарта Республики Узбекистан на Алгоритм шифрования данных и Функцию хэширования. // Информационная безопасность в сфере связи и информатизации: Тезисы доклодов республиканского семинара 24 ноября 2005. – Ташкент. – С. 77-80.

6. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Дастлабки ва формал криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №1 (4). – 32-37 бетлар.

7. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Илмий криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №2 (5). – 47-53 бетлар.

8. Ахмедова О.П. Уч параметрли бир томонлама функциялар ва уларнинг хоссалари // ТошДТУ хабарлари. – Тошкент, 2006, №2. – 46-48 бетлар.

9. Ахмедова О.П. Усовершенствованные алгоритмы электронной цифровой подписи К. Шнорра // Кимёвий технология. Назорат ва бошқарув. – Тошкент, 2006, №4. – С. 83-87.

10. Назаров Х.Н., Ахмедова О.П. Носимметрик криптографик тизимлар // ТошДТУ хабарлари – Тошкент, 2006, №3. – 26-28 бетлар.

11. Ахмедова О.П. Аналог схемы электронной цифровой подписи К. Шнорра в алгебре с параметром // Международная научно-практическая конференция. «Актуальные проблемы использования электронной цифровой подписи» 24-25 мая 2006 г. Доклады и тезисы. – Ташкент. – С. 64-67.

12. Исаев Р.И., Хасанов П.Ф., Хасанов Х.П., Мазгаров Б.А., Ахмедова О.П. О государственном стандарте РУз O'z Dst 1092:2005. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи // Международная научно-практическая конференция. «Актуальные проблемы использования электронной цифровой подписи» 24-25 мая 2006 г. Доклады и тезисы. – Ташкент. – С. 18-20.

13. Ахмедова О.П. Уч параметрли бир томонлама функциялар асосида яратилган носимметрик криптографик алгоритмлар // Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Муаммолар ва уларни ҳал этиш йўллари. Республика семинари, CD-диск (Тошкент ш. 18 октябрь 2006 й.).

14. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Ахмедова О.П. О государственном стандарте Узбекистана «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – С. 36-48.

15. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – 59-74 бетлар.

16. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Ахмедова О.П. О государственном стандарте Республики Узбекистан на алгоритм шифрования данных // Aloqa dunyosi. – Тошкент, 2007, №1 (7).– 57-71 бетлар.

Ҳаммуаллифликдаги IAP 03070-сон патентида даража асосининг махфийлиги ғояси, бошқа мақола ва маърузаларда эса криптографиянинг ривожланиши даврларига оид маълумотлар таҳлили, носимметрик криптотизимларнинг қиёсий таҳлилига ва ва таснифига оид маълумотлар, стандартларда фойдаланилган атамалар ва уларнинг таърифларига оид маълумотлар, стандартларнинг математик таъминоти баёни, тадқиқотнинг умумий вазифаларига оид маълумотлар муаллифга тегишлидир.

Техника фанлари номзоди илмий даражасига талабгор Ахмедова Ойдин Пўлатовнанинг 05.13.19 – «Ахборотлар технологияси, ахборотлар хавфсизлигини таъминлаш тизимлари ва усуллари» ихтисослиги бўйича «Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари» мавзусидаги диссертациясининг

РЕЗЮМЕСИ

Таянч сўзлар: алгоритм, носимметрик, криптотизим, электрон рақамли имзо, калит, ошкора калит, бардошлилик, параметр, усул, алгебра, бир томонлама функция.

Тадқиқот объектлари: мавжуд носимметрик криптотизимлар яратиш усули ва алгоритмлари.

Ишнинг мақсади: параметрлар алгебраси асосида носимметрик криптоалгоритмлар яратиш усули ва бу усулга асосланган бардошли криптоалгоритмлар ишлаб чиқиш.

Тадқиқот усули: информатика асослари, алгебраик структуралар, носимметрик криптографик тизимлар ва параметрли алгебра усуллари.

Олинган натижалар ва уларнинг янгилиги:

- носимметрик криптотизимларнинг муаммо тури бўйича таснифи;
- параметрлар алгебраси;
- уч параметрли яшириш йўлли бир томонлама функция;
- параметрлар алгебрасида носимметрик криптографик алгоритмлар яратиш усули;
- бардошлилиги даража параметрлари учлиги муаммосининг мураккаблигига асосланган электрон рақамли имзо ва шифрлаш алгоритмлари.

Амалий аҳамияти: ишлаб чиқилган криптоалгоритмлар мавжуд криптотизимларга нисбатан бардошлилиги юқори бўлган криптотизимлар ишлаб чиқишда ва ўқув муассасаларида ахборот хавфсизлиги бўйича кадрлар тайёрлаш жараёнида қўлланилиши мумкинлиги билан аҳамиятга эга.

Татбиқ этиш даражаси ва иқтисодий самарадорлиги: диссертация давомида олинган натижалардан ахборотнинг криптографик муҳофазаси бўйича Ўзбекистон давлат стандартлари ишлаб чиқишда, муҳофазаланган электрон почта E-ХАТ тизимида ва ЎзААА ФТМТМ ахборот хавфсизлиги ва криптология йўналиши бўйича илмий ҳисоботларда фойдаланилган.

Қўлланиш соҳаси: диссертация иши натижаларидан республикамизнинг ахборот ва коммуникация тизимларида ва ўқув муассасаларида фойдаланилиш мумкин.

РЕЗЮМЕ

диссертации Ахмедовой Ойдин Пулатовны на тему «Способ и алгоритмы создания асимметричных криптосистем на основе алгебры параметров» на соискание ученой степени кандидата технических наук по специальности 05. 13. 19 – «Информационные технологии, методы и системы обеспечения информационной безопасности».

Ключевые слова: алгоритм, асимметричная криптосистема, электронная цифровая подпись, ключ, открытый ключ, стойкость, параметр, способ, алгебра, односторонняя функция.

Объекты исследования: способы и алгоритмы создания существующих асимметричных криптосистем.

Цель работы: разработка способа и алгоритмов создания стойких асимметричных криптосистем на основе алгебры параметров.

Метод исследования: основы информатики, алгебраические структуры, методы асимметричных криптографических систем и алгебры параметров.

Полученные результаты и их новизна:

- классификация асимметричных криптосистем по типу решаемых проблем;
- алгебра параметров;
- односторонняя функция с секретом из трех параметров;
- способ создания асимметричных криптосистем на основе алгебры параметров;
- алгоритмы электронной цифровой подписи и шифрования, стойкость которых основана на сложности проблемы тройки параметров степени.

Практическая значимость: разработанные криптоалгоритмы могут быть использованы в процессах разработки криптосистем, обладающих по сравнению с известными повышенной стойкостью, а также в процессах подготовки кадров в учебных заведениях по информационной безопасности.

Степень внедрения и экономическая эффективность: результаты, полученные в диссертации, использованы в процессе разработки государственного стандарта Узбекистана по криптографической защите информации, в системе защищенной электронной почты E-XAT и в научных отчетах по направлениям информационной безопасности и криптологии ЦНТМИ УзАСИ.

Область применения: результаты, полученные в диссертации, могут быть использованы в информационных и коммуникационных системах республики и в процессах обучения в высших учебных заведениях.

RESUME

Thesis of Akhmedova Oydin Polatovna on the scientific degree competition of candidate of science in 05. 13. 19 speciality «Information technologies, methods and information security providing systems» subject: «Creation methods and algorithms of asymmetrical crypto systems on base algebra of parameters».

Key words: algorithm, asymmetrical cryptosystem, digital signature, key, public key, resistance, parameter, method, algebra, one way function.

Subjects of the inquiry: creation methods and algorithms of existing asymmetrical crypto systems.

Aim of the inquiry: development creation methods and algorithms of firm asymmetrical cryptosystems on base algebra of parameters.

Method of inquiry: base of informatics, algebraic structures, methods of asymmetrical crypto systems and algebra of parameters.

The results achieved and their novelty:

- classification of asymmetrical crypto systems by type of resolving problem;
- algebra of parameters;
- one-way function with secret;
- creation methods of asymmetrical crypto systems on base algebra of parameters;
- formation of problem of three power parameters;
- Digital Signature and ciphering algorithms resistance of which based on complexity of three power parameters problem.

Practical value: developed crypto algorithms can be used in process of developing crypto systems which have high resistance relatively existing algorithms and in applying in cryptography discipline during process of preparation specialists at the educational institutions by information security.

Degree of embed and economic affectivity: results, gotten in dissertation applied in developing governmental standard of Uzbekistan by information protection with using cryptography, protected electronic mail system E-XAT and in scientific reports of carried out scientific-research works of Communication and information agency of Uzbekistan by directions of information security and cryptology.

Sphere of usage: results gotten in dissertation count of much in using in information and communication systems of republic and in educational institutions.

Босишга рухсат этилди 24.04.2007 й. Бичими 60x84 1/16.
Шартли босма табоғи 1. Нусхаси 100 дона. Буюртма № 215.

ТДТУ босмахонасида чоп этилди. Тошкент ш,
Талабалар кўчаси 54. тел: 396-63-84.