КОМПЬЮТЕРНЫЕ НАУКИ, ПРИБОСТРОЕНИЕ И АВТОМАТИЗАЦИЯ
КОМПЬЮТЕРЛІК ҒЫЛЫМДАР, АСПАП ЖАСАУ ЖӘНЕ АВТОМАТТАНДЫРУ
COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION

ӘӨЖ 004.056
ҒТАХА 81.93.29
https://doi.org/10.53364/24138614_2026_41_2_11

Қ.С. Сақан[1,2], К.Т. Алғазы[1*], А.В. Варенников[1], А.Ж. Абишева[3]

Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан
әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан

E-mail: kunbolat@mail.ru

VERKLE АҒАШЫНА НЕГІЗДЕЛГЕН ЦИФРЛЫҚ ҚОЛТАҢБАНЫҢ ТИІМДІЛІГІН БАҒАЛАУ ЖӘНЕ САЛЫСТЫРМАЛЫ ТАЛДАУ ЖҮРГІЗУ

Аңдатпа. *Мақалада қытайдың қалдықтар теоремасын қолдана отырып, Verkle ағашына негізделе ұсынылған цифрлық қолтаңбаның тиімділігін эксперименттік бағалау зерттелген. Кілттерді құру, қолтаңбаны қалыптастыру және оны тексеру алгоритмдерін бағдарламалық қамтамасыз ету әзірленді. Ұсынылған схемада, Verkle ағашы міндеттемелерді ықшамды түрде көрсету үшін қолданылады, ал қытайдың қалдықтар теоремасы модульдік есептеулерді оңтайландыру және қолтаңба жасау мен тексеру операцияларының есептеу тиімділігін арттыру үшін қолданылады. Алгоритмдердің уақыт бойынша сипаттамаларына талдау жасалды, сонымен қатар, күрделілік көрсеткіштері көрсетілді. Статистикалық сенімділікті қамтамасыз ету үшін, эксперименттік нәтижелер көпретті сынақтар жүргізетін бекітілген есептеу платформасында алынды. Құрылған қолтаңба алгоритмінің негізгі параметрлері мен орындалу уақыты бойынша Kate-Zaverucha-Goldberg (KZG) көпмүшелік міндеттемелерінің классикалық схемасының цифрлық қолтаңбасымен салыстырмалы талдау жасалды. Алынған нәтижелер Verkle ағашына қытайдың қалдықтар теоремасын қолдана отырып цифрлық қолтаңбаларды құру перспективалы бағыт екенін көрсетеді.*

Түйін сөздер: *Verkle ағашы, векторлық міндеттеме, көпмүшелік міндеттеме, қытайдың қалдықтар теоремасы, цифрлық қолтаңба, аутентификация, тексеру.*

Кіріспе.

Цифрлық технологиялардың дамуы және берілетін ақпарат көлемінің өсуі деректердің түпнұсқалығы мен тұтастығын қамтамасыз ету тетіктерін жетілдіру қажеттілігін тудырады. Цифрлық қолтаңба хабарлама көзінің түпнұсқалығын растауды және рұқсат етілмеген өзгерістерден қорғауды қамтамасыз ететін негізгі криптографиялық құралдардың бірі болып табылады. Кванттық есептеулердің қолдану болашағын ескере отырып, есептеу технологияларының қарқынды дамуы жағдайында өнімділігі жоғары және ықшамды цифрлық қолтаңбаның тиімді схемаларын әзірлеу міндеті өзекті болып отыр.

Crystals-Dilithium, Falcon және SPHINCS+ сияқты заманауи цифрлық қолтаңба схемалары криптографиялық беріктіліктің жоғары деңгейін көрсетеді. Бірақ бұл алгоритмдерде кілттер мен қолтаңбалардың көлемі едәуір үлкен және есептеу шығындары жоғары болып табылады. Осыған байланысты зерттеудің өзекті бағыты ретінде берілетін деректер көлемін азайтуды және есептеу операцияларын оңтайландыруды қамтамасыз ететін балама құрылымдық шешімдерді іздеуді атауға болады.

Перспективалы бағыттардың бірі болып Verkle құрылымы табылады, яғни векторлық міндеттемелерге негізделген құрылым. Бұл элементтің сәйкестігін дәлелдеудің логарифмдік күрделілігін және криптографиялық растаудың ықшамдылығын қамтамасыз етеді. Қытайдың қалдықтар теоремасын (ҚҚТ) қолдану – модульдік операцияларды ыдыратуға және арифметикалық есептеулердің тиімділігін арттыруға мүмкіндік беретін есептеулерді оңтайландырудың қосымша мүмкіндіктерін қамтамасыз етеді.

Бұл жұмыстың негізгі мақсаты қытайдың қалдықтар теоремасын қолдана отырып, Verkle ағашына негізделген цифрлық қолтаңбаны бағдарламалық қамтамасыз етуді әзірлеу, оның тиімділігіне эксперименттік бағалау жүргізу және заманауи цифрлық қолтаңба схемаларымен салыстырмалы талдау жасау болып табылады.

Жұмыстың ғылыми жаңалығы ҚҚТ қолдана отырып, Verkle ағашына негізделген цифрлық қолтаңбаны бағдарламалық қамтамасыз етуді әзірлеу және эксперименттік зерттеу болып табылады. Verkle ағашы мен модульдік арифметиканы оңтайландыру әдістері негізінен бөлек қарастырылатын қолданыстағы зерттеулерден айырмашылығы, бұл жұмыс оларды цифрлық қолтаңбаның бірыңғай алгоритмдік моделі шеңберінде біріктіруді ұсынады.

Зерттеудің практикалық маңыздылығы, Verkle ағашына негізделген құрылымдарда ҚҚТ бағытталған есептеулердің тиімділігін бағалауға мүмкіндік беретін бағдарламалық құралды құру болып табылады. Әзірленген бағдарламалық жасақтаманы ықшамды криптографиялық хаттамаларды құру саласындағы қосымша зерттеулер үшін, сондай-ақ үлкен сандармен жұмыс істеу кезінде модульдік арифметиканы оңтайландыруды қажет ететін жүйелерді жобалау үшін пайдалануға болады.

Айта кететіні – зерттеуде Verkle ағашы мен ҚҚТ-на негізделген модульдік арифметиканы цифрлық қолтаңбаның алгоритмдік моделіне интеграциялау басты ұстаным болды. Ұсынылған тәсіл міндеттемелерді қалыптастыру, дәлелдемелерді генерациялау және тексеру процестерін біртұтас схема ретінде қарастыру және белгілі бір криптографиялық тәсілдерді біріктіріп ғана қоймай, оларды нақты цифрлық қолтаңба схемасы ретінде формализациялау, бағдарламалық іске асыру және оның тиімділігін тәжірибелік түрде дәлелдеу іске асырылды.

Жоғары дәрежелі полиномдармен Галуа өрісінде операциялар орындау, әсіресе олардың көбейту бойынша кері элементін табу – есептеу жағынан күрделі және ресурсты қажет ететін процесс. Бұған қоса, полиномдардың примитивті полином екендігін тексеру (дәлелдеу) процедурасы да есептеу шығындарының артатыны белгілі. Осыған байланысты, аталған операциялардың тиімділігін арттыру мақсатында оңтайландырылған тәсілдер пайдаланылды.

Әдебиеттерге шолу.

Заманауи цифрлық қолтаңба схемаларын әзірлеу және оларды талдау постквантты криптографияға көшуге кезеңінде белсенді дамып келеді. Ең маңызды бағыттардың бірі – постквантты алгоритмдерді стандарттау бойынша Американың Ұлттық стандарттар және технологиялар институты (ҰСТИ) байқауы аясында іріктеуден өткен қолтаңбаның торлы схемалары. Атап айтқанда, Module-LWE және Module-SIS есептерінің қиындықтарына негізделген Crystals-Dilithium алгоритмінің [1] қолтаңба сипаттамасы болып табылады. Жұмыста кілттерді құру алгоритмдерінің ресми анықтамалары, қолтаңбаны қалыптастыру және тексеру, қауіпсіздік параметрлерінің негіздемесі, сондай-ақ іске асырудың практикалық аспектілері келтірілген. Сонымен бірге, есептеу күрделілігін бағалауға және кілттер мен қолтаңбалардың өлшемдеріне айтарлықтай назар аударылады. Бұл жұмыс эксперименттік өлшеулер жүргізу және өнімділік сипаттамаларын салыстырмалы талдау үшін әдіснамалық бағдар береді және жаңа цифрлық қолтаңба схемаларын қолданыстағы стандарттармен салыстыру кезінде маңызды.

Криптографиялық құрылымдарды құрудың балама тәсілдері жетілдірілген міндеттеме ағаштарын пайдаланумен байланысты. М. Явич және басқа да бірлескен авторлардың

жұмысы [2] Verkle ағашын постквантық цифрлық қолтаңба бағытында қолдануды қарастырады. Авторлар классикалық Меркла ағашымен салыстырғанда аталған құрылымның ерекшеліктерін талдайды және оның векторлық міндеттемелерді пайдалану және жоғары тармақталу арқылы тиесілілік дәлелінің мөлшерін азайтудағы артықшылығын атап көрсетеді. Зерттеуде алгоритмдік схеманың сипаттамасын береді және көлемін өзгерту мәселелерін талқылайды. Verkle құрылымдары ағаштың тереңдігін едәуір қысқартуға және сәйкесінше тексеру кезінде растайтын ақпарат көлемін азайтуға мүмкіндік беретіні көрсетілген. Бұл нәтижелер Verkle ағашын ықшам және жоғары өткізу қабілеттілігіне бағытталған жүйелерде қолдану мүмкіндігін көрсетеді.

Криптографиялық алгоритмдердегі арифметикалық амалдарды оңтайландыру мәселелері дәстүрлі түрде ҚҚТ қолданумен байланысты. Khalfin шолуында [3] ҚҚТ-ны криптографияда қолданудың негізгі бағыттарын, соның ішінде RSA (Rivest-Shamir-Adleman) тәрізді тізбектердегі есептеулерді жеделдетуді, құпия жүйелерді құруды және күрделі есептеу операцияларының модульдік ыдырауын қарастырады. Автор ҚҚТ қолдану үлкен модуль бойынша есептеулерді өзара қарапайым модульдер бойынша параллель операциялар жиынтығымен ауыстыруға, содан кейін нәтижені қайта құруға мүмкіндік беретінін атап көрсетеді. Бұл тәсіл үлкен сандармен жұмыс жасағанда есептеу шығындарын азайтады және алгоритмдерді іске асырудың тиімділігін арттырады. Бұл жағдайда, теорема қауіпсіздіктің тәуелсіз криптографиялық алғышарты ретінде емес, оңтайландыру құралы ретінде қарастырылады. Бұл ережелер ҚҚТ-ын векторлық міндеттемелерге негізделген құрылымдарға біріктірудің әдіснамалық негізі болып табылады.

ҚҚТ-ны криптографиялық есептеулерде практикалық қолданудың маңызды мысалы-Grossschädl жұмысы. Бұл жұмыста RSA чипі ҚҚТ-оңтайландырылуымен аппараттық енгізу модульдік көрсеткішті екі параллель ішкі тапсырмаға бөлу арқылы шифрды ашу операциясын шамамен 3.5 есе жеделдетуге қол жеткізеді [4]. Бұл тек теориялық құрал ретінде ғана емес, сонымен қатар Verkle негізіндегі қолтаңба схемаларында есептеулерді оңтайландыруға да тікелей қатысы бар криптографиялық алгоритмдердің өнімділігін арттырудың нақты әдісі ретінде қызмет ете алатынын көрсетеді. RSA чиптеріндегі модульдік операцияларды қалай жылдамдататынына ұқсас, Verkle ағаштарында ҚҚТ модульдік есептеулерді оңтайландыру үшін қолданылуы мүмкін, бұл міндеттемелерді қалыптастыру мен тексеруге кететін уақытты азайтады.

Кейбір зерттеулер ҚҚТ қолдану модульдік арифметиканың негізгі операцияларын тиімді жеделдетеді деп санайды. RSA-алгоритмді оңтайландыру бойынша эксперименттік жұмыстарда ҚҚТ-оңтайландырылған RSA нұсқасы есептеулерді кіші модульдер бойынша параллель ішкі тапсырмаларға бөлудің және нәтижені кейіннен қайта құрудың арқасында n модулі бойынша дәрежеге шығару классикалық операциялардан шамамен 3-4 есе жылдам орындайтынын көрсетеді [5]. Бұл оның криптографиялық есептеулердің өнімділігін арттырудың инженерлік құралы ретіндегі практикалық пайдалылығын дәлелдейді және Verkle құрылымындағы векторлық міндеттеме операцияларын оңтайландыру үшін де осылай қолдануға болады. Құрылымында үлкен модульдік есептеулері бар криптографиялық жүйелер үшін (соның ішінде векторлық міндеттемелерге негізделген схемалар) ҚҚТ қолдану арифметикалық амалдардың өнімділігін айтарлықтай оңтайландыруға мүмкіндік береді. Бұл қолтаңба мен тексеруді жүзеге асырудың тиімділігіне тікелей әсер етеді.

Постквантық алгоритмдердің өнімділігін салыстырмалы зерттеу бірқатар заманауи зерттеулерде ұсынылған. Demir және бірлескен авторлардың мақаласы [6] постквантық криптография алгоритмдерін өнеркәсіптік енгізудің тиімділігі мен мүмкіндіктерін саралайды. Авторлар кілт генерациясының, қолтаңбаның және тексерудің уақыт сипаттамаларын зерттейді және алгоритмдердің шектеулі платформаларға әсерін бағалайды. Әр түрлі схемалар қолтаңба өлшемі мен есептеу жүктемесі арасындағы әр түрлі тепе-теңдікті көрсетеді. Бұл салыстырмалы талдауды жаңа шешімдерді әзірлеудің міндетті

кезеңіне айналдырады. Көрсетелген нәтижелер криптографиялық қауіпсіздік параметрлерін сақтай отырып, инженерлік оңтайландырудың маңыздылығын көрсетеді. Бұл тәсіл нақты есептеу жағдайында жаңа схемалардың тиімділігін эксперименттік бағалау қажеттілігін көрсетеді.

Ұсынылған зерттеулер көрсеткендей, қолданыстағы жұмыстар постквантық цифрлық қолтаңба схемаларын әзірлеу мен стандарттауды, міндеттеме құрылымдарын зерттеуді немесе ҚҚТ көмегімен арифметиканы оңтайландыру мәселелерін қамтиды. Алайда, ғылыми әдебиеттерде Verkle ағашының құрылымын және цифрлық қолтаңба схемасын эксперименттік іске асыру шеңберінде ҚҚТ қолдануды біріктіретін кешенді зерттеулер шектеулі. Сонымен бірге, олардың қазіргі заманғы постквантық алгоритмдерге қатысты тиімділігін салыстырмалы талдаулар да аз. Бұл осы зерттеудің өзектілігін анықтайды және оның ғылыми жаңалығын қалыптастырады.

Жұмыстың негізгі үлесі.

Бұл жұмыстың негізгі үлесі төмендегідей:

1. Қытай қалдықтары теоремасына негізделген көпмүшелік міндеттемелерді Verkle ағашының құрылымына біріктіру. Көпмүшелік міндеттемелердің негізгі схемасы қарастырылған авторлардың алдыңғы жұмыстарынан айырмашылығы, бұл мақалада оның бейімделуі және Verkle ағашының иерархиялық құрылымында қолданылуы ұсынылған, бұл деректердің тиесілігін тиімді ұсынуға және тексеруге мүмкіндік береді.

2. Цифрлық қолтаңбаның толық алгоритмдік моделін жасау. Криптографиялық хаттаманың толықтығын қамтамасыз ететін кілттерді құру (KeyGen), міндеттемелерді қалыптастыру (Commit), ашу (Open), тексеру (Verify) және жаңарту (Update) процедураларын қамтитын тұтас схема ұсынылған.

3. Ұсынылған схеманы бағдарламалық қамтамасыз ету (VCNPSS v1. 0). NTL және GMP кітапханаларын қолдана отырып, барлық негізгі криптографиялық процедураларды жүзеге асыратын бағдарламалық жасақтама жасалды, бұл алгоритмнің сипаттамаларын практикалық тестілеуге және талдауға мүмкіндік береді.

4. Есептеу тиімділігін эксперименттік бағалау. n қауіпсіздік параметрлеріне және k құрылымының өлшеміне байланысты алгоритмнің уақыт сипаттамаларына егжей-тегжейлі талдау жүргізілді, бұл күрделіліктің теориялық бағаларын растайды және ұсынылған тәсілдің масштабталуын көрсетеді.

5. KZG полиномдық міндеттемелерінің классикалық схемасымен салыстырмалы талдау. Негізгі параметрлер бойынша салыстыру жүргізілді (есептеу күрделілігі, дәлелдемелер құрылымы, іске асыру ерекшеліктері), Бұл ұсынылған схеманың эллиптикалық қисықтар мен екі сызықты карталарды пайдаланбай балама шешім ретінде қолдану аймағын анықтауға мүмкіндік береді.

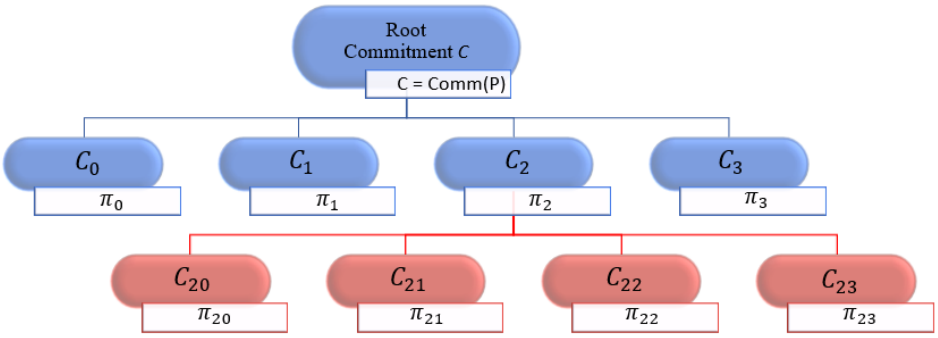
6. Бұрын жарияланған нәтижелерді дамыту. Бұл жұмыс ұсынылған әдістің теориялық негіздері қаланған [7,8] авторлардың зерттеулерінің жалғасы болып табылады. Аталған жұмыстардан айырмашылығы, осы мақалада Verkle құрылымдарымен интеграцияға, бағдарламалық жасақтаманы іске асыруға және эксперименттік валидацияға баса назар аударылады.

Зерттеу материалдары мен әдістері.

Меркл ағашы. Меркл ағашы – бұл Ральф Меркл ұсынған классикалық криптографиялық құрылым. Ол тұтастықты қамтамасыз етуге және деректердің берілген жиынтыққа жататындығын тиімді тексеруге арналған. Ағаштың құрылымы хэш мәндерінің иерархиялық ұйымдастырылуына негізделген. Ағаш жапырақтарында бастапқы деректердің хэштері бекітіледі, ал ішкі түйіндер еншілес төменгі екі түйіннің мәндерін тіркескен жазбасын хэштеу арқылы қалыптасады. Түбірлік мән (Merkle root) бүкіл деректер жиынтығы үшін криптографиялық міндеттеме ретінде қызмет етеді. Меркл ағашының басты артықшылығы – элементтің тиесілігін дәлелдеудің логарифмдік күрделілігі, ал

дәлелдеменің мөлшері ағаштың биіктігіне тура пропорционалды екендігінде. Дегенмен, деректер көлемі ұлғайған сайын Меркл ағашының тереңдігі артады, бұл дәлелдеме өлшемінің ұлғаюына және тексеру кезінде хэш операцияларының санының артуына әкеледі. Үлкен көлемді өңдеу мен ықшамдылықты қажет ететін есептерде бұл шектеуші фактор болуы мүмкін.

Сол себепті, Меркл ағашын жалпыламасы болып табылатын векторлық міндеттемелерді қолданатын Verkle ағашының құрылымы осыған балама ретінде ұсынылды. Бұл құрылымның екілік иерархиядан айырмашылығы Verkle ағашы жоғары санды тармақталуға мүмкіндік береді және бір түйінде бірнеше мәндерді біріктіру үшін криптографиялық векторлық міндеттемелерді пайдаланады (Сурет 1). Бұл ағаштың биіктігін едәуір азайтуға және элементке жататындығын тиімдірек дәлелдеуге мүмкіндік береді. Нәтижесінде тексерудің (верификацияның) логарифмдік күрделілігін сақтай отырып, деректерді жинақты бейнелеуге қол жеткізіледі.



Сурет 1 – Verkle ағашының құрылымдық сұлбасы

Verkle ағашын цифрлық қолтаңба схемасында қолдану растауды қажет ететін ақпарат көлемінің азаюын қамтамасыз етеді және тексеру кезінде есептеу операцияларының санын азайтады. Қытайдың қалдықтар теоремасына негізделген модульдік есептеулерді оңтайландырумен біріктірілген бұл құрылым тиімді және үлкен көлемді есептерге бейімделген криптографиялық құрылымның негізін құрайды.

Қытайдың қалдықтар теоремасы әртүрлі модульдермен сызықтық салыстырулар жүйелерін шешу үшін қолданылатын сандар теориясының негізгі инструменттерінің бірі деп қарастыруға болады. Теореманың негізгі мәні мынада: егер $m_1, m_2, \dots, m_n$ модульдері өзара жай болатын болса, онда кез-келген $a_1, a_2, \dots, a_n$ бүтін сандар жиынтығы үшін $x \equiv a_i (mod\ m_i),\ i = 1,2, \dots, n$ салыстырулар жүйесін қанағаттандыратын және $M = \prod_{i=1}^{n} m_i$ модульдік мәні дәлдігімен анықталатын *x* саны бар болады және ол жалғыз болады. Басқаша айтқанда, модульдер өзара жай болғанда салыстырулар жүйесінің шешімі бар болады және ол шешім *M* қалыңдылар сақинасында жалғыз болады [7].

Теореманың практикалық маңыздылығы есептеулерді үлкен модуль бойынша операциялардың жиынтығын кішігірім өзара қарапайым модульдер бойынша ыдырату, содан кейін жалпы нәтижені қайта құру мүмкіндігі болып табылады. Бұл тәсіл үлкен биттік сандармен жұмыс істеу кезінде есептеу шығындарын едәуір азайтуға мүмкіндік береді. Осы себепті қытайдың қалдықтар теоремасы криптографиялық алгоритмдерде, цифрлық сигналдарды өңдеуде және ақпаратты кодтау жүйелерінде кеңінен қолданылады [8].

Шешімді құру процедурасы әдетте бірнеше тізбектелген қадамдарды қамтиды. Алдымен жиынтық модулі $M = \prod_{i=1}^{n} m_i$ анықталады. Содан кейін әрбір салыстыру үшін $M_i = \frac{M}{m_i}$ ішінара модулі есептеледі. Әрі қарай, әрбір i үшін $M_i \cdot y_i \equiv 1 (\mathrm{mod} m_i)$ шартын

қанағаттандыратын y_i мультипликативті кері элементі есептелінеді. Жүйенің шешімі $x = \sum_{i=1}^{n} a_i M_i y_i$ сызықтық комбинациясы ретінде қалыптасады, қажет болған жағдайда M үлкен модулі бойынша беріледі.

Осы құрылым шеңберіндегі есептеу операцияларын оңтайландыру қытайдың қалдықтар теоремасын қолдану арқылы одан әрі де жүргізілуі мүмкін. Теорема M үлкен модуль бойынша есептеулерді өзара жай модульдерге қатысты параллель есептеулер жиынтығы түрінде ұсынуға, содан кейін нәтижені қайта құруға мүмкіндік береді. Verkle ағашының құрылымында бұл векторлық міндеттемелерді қалыптастыруға және тексеруге байланысты арифметикалық амалдарды ыдыратуға мүмкіндік береді, бұл дәлелдемелерді жинақы ұстай отырып, есептеу шығындарын азайтады.

Нәтижелері және оларды талқылау.

Зерттеу барысында қытайдың қалдықтар теоремасын пайдалана отырып, Verkle ағашы құрылымындағы полиномдық міндеттемелерге негізделген цифрлық қолтаңбаның бағдарламалық моделі жасалынды. Алгоритмдік схема кілттерді құру (KeyGen), міндеттемелерді қалыптастыру (Com), дәлелдемені ашу (Open), міндеттемені тексеру (Ver), міндеттемелер мен дәлелдемелерді жаңарту (Update, ProofUpdate) процедураларын қамтиды.

Бастапқы параметрлер.

Алгоритмді бағдарламалық деңгейде дұрыс іске асыру үшін алдымен схеманың жұмыс істеуін қамтамасыз ететін бастапқы параметрлер мен деректер құрылымдарының жиынтығын анықтап, қалыптастыру қажет. Мұндай параметрлердің қатарына полиномдардың дәрежесін және шығыс хэш мәнінің ұзындығын анықтайтын n қауіпсіздік параметрінің мәні, Verkle ағашының құрылымындағы k түйіндерінің саны, берілген дәрежедегі жұп-өзара қарапайым $p_i(x)$ келтірілмейтін полиномдар жиынтығы, сондай-ақ жалғанкездейсоқ тізбектер генераторы жасаған $g_i(x)$ кілттерінің жиынтығы жатады. Оларды анықтау тәртібі:

1) n – қауіпсіздік параметрін анықтау, екілік жазбада ұсынылған кезде n полиномның дәрежесін немесе оның ұзындығын анықтайды.

2) $k \in N$ параметрін анықтау, бұл – Verkle ағашындағы түйіндер саны.

3) Толық $G(x) = \big(g_1(x), g_2(x), \dots, g_k(x)\big)$ кілтін құрайтын $g_i(x)$ құпия кілттерін қажетті мөлшерде қалыптастыру үшін қажетті $\mathbb{G}$ жалғанкездейсоқ тізбектер генераторын пайдалану, мұндағы $def\big(g_i(x)\big) = n$ және $g_1(x) \neq g_2(x) \neq \cdots \neq g_k(x), i = 1..k$.

4) Дәрежесі $n+1$ болатын келтірілмейтін полиномдардың $\mathbb{P}$ жиыны болуы керек. Берілген жиыннан $p_i(x)$ полиномдары кездейсоқ түрде $p_1(x) \neq p_2(x) \neq \cdots \neq p_k(x),\ i = 1..k$ ескеріліп таңдалады. Олар позициялық емес полиномиялдық санау жүйесінің жұмыс негіздері ретінде қарастырылатын болады.

5) Деректерді хэштеу үшін кез-келген криптографиялық берік хэш функция $H: \{0,1\}^* \to \{0,1\}^n$ қолданылады. Біздің жағдайда, деректерді хэштеу үшін алдын-ала әзірленген LWH-512 алгоритмінің бағдарламалық жасақтамасы қолданылды. LWH-512 таңдалуы оның коллизиялық шабуылдарға, алғашқы түпбейнеге, екінші алғашқы түпбейнеге бағытталған шабуылдарға төзімділігіне, сондай-ақ лавиндік әсеріне және тұрақты статистикалық сипаттамаларына байланысты болды [9]. $\pi_i(x)$ дәлелдерді қалыптастыру және Verkle ағашының құрылымындағы көпмүшелік міндеттемелерді есептеу кезінде ұзындығы 512 битті шығыс мәнін пайдалану криптографиялық төзімділіктің қажетті деңгейін қамтамасыз етеді.

6) $P_i^{-1}(x)$ мультипликативті кері полиномды $p_i(x)$ модулімен есептеу үшін кеңейтілген Евклид алгоритмі (КЕА) қолданылады.

Бағдарлама жасау үшін алгоритм.

Төменде полиномдық міндеттемелерге және ҚҚТ негізделген ұсынылған цифрлық қолтаңба схемасын бағдарламалық қамтамасыз ету алгоритмі берілген. Алгоритм бес кезеңнен тұрады: кілттерді жасау, міндеттемелер мен дәлелдемелерді қалыптастыру, жариялау, тексеру (верификациялау) және Verkle ағаш құрылымындағы деректерді жаңарту қадамдары.

1) *Кілттерді жасау кезеңі* – $\mathrm{KeyGen}(1^n, k)$

1.1) $\mathbb{G}$ псевдокездейсоқ тізбектер генераторын пайдаланып, $G(x) = \big(g_1(x), g_2(x), \dots, g_k(x)\big)$ толық кілтті құрайтын қажетті мөлшердегі $g_i(x)$, $i = 1..k$ кілттерін жасау.

1.2) $\mathbb{P}$ жиынынан $p_i(x)$, $i = 1..k$ таңдап алу.

2) *Міндеттемелер мен дәлелдемелер қалыптастыру кезеңі* – $Com_{pp}(m_1(x), \dots, m_k(x))$

2.1) Берілген $m_i(x)$ арқылы $h_i(x) = H(m_i(x))$, $i = \overline{1,k}$ есептеу.

2.2) Есептеу $\pi_i(x) = h_i(x) \oplus g_i(x)$, $i = \overline{1,k}$. Ескере кететіні, $deg\big(g_i(x)\big) = deg\big(h_i(x)\big) = n$.

2.3) Қытайдың қалдықтар теоремасын пайдаланып, $C(x)$ міндеттемесін есептеу. Ол үшін:

1. Есептеу $P(x) = \prod_{i=1}^{k} p_i(x)$.
2. Есептеу $P_i(x) = \frac{P(x)}{p_i(x)}$, $i = \overline{1,k}$.
3. КЕА пайдаланып және $P_i(x) \cdot P_i^{-1}(x) \equiv 1 \ (mod\ p_i(x))$, $i = \overline{1,k}$ ескере отырып, $P_i^{-1}(x)$ есептеу.
4. Міндеттемені есептеу – $C(x) = \sum_{i=1}^{k} \pi_i(x) \cdot P_i(x) \cdot P_i^{-1}(x)\ mod\ P(x)$ және оны деректерді растау үшін ашық кілт ретінде жариялау.

3) *Жариялау кезеңі* – $Open(m_i(x), \pi_i(x), i)$.

Алгоритм $m_i(x)$ хабарламасының $\pi_i(x)$ міндеттемесі бар екенін және бұл міндеттеме басқа $\pi_j(x)$ ($i \neq j$) мәндерін ашпай-ақ $C(x)$ дәлелдемесінің құрамына кіретінін жариялайды.

4) *Верификациялау кезеңі* – $Ver(C(x), p_i(x), g_i(x), i)$.

Алгоритм берілген міндеттеме $\pi_i(x)$ шынымен $C(x)$ ішінде қатысқанын және сәйкесінше қол қойылған немесе қабылданған $m_i(x)$ хабарламасы өзгертілмегенін тексереді. Ол үшін $(p_i(x), g_i(x))$ дәлелдемелері жіберіледі және келесі есептеулер жасалады және олардың нәтижелері салыстырылады:

4.1) Есептеу $\pi_i(x) = C(x)\ mod\ p_i(x)$, $i = \overline{1,k}$.

4.2) Есептеу $y_i(x) = H(m_i(x)) \oplus g_i(x)$, $i = \overline{1,k}$.

4.3) Егер $\pi_i(x) = y_i(x)$, онда міндеттеме ақиқат сәйкесінше, m_i хабарламасы нақты осы және өзгермегендігі расталады.

5) *Жаңарту кезеңі* – $Update(C(x), m_i(x), m_i'(x), g_i'(x), i)$.

Алгоритмді жіберуші i-ші хабарламаны ауыстыру арқылы $C(x)$ міндеттемесін жаңартқысы келеді. Жаңарту үшін міндеттеме келесідегідей қайта есептеледі: $C'(x) = \sum_{i=1}^{k} \pi_i'(x) \cdot P_i'(x) \cdot {P_i'}^{-1}(x)\ mod\ P(x)$, $i = \overline{1,k}$. Бұл жағдайда $P(x)$ қайта есептеудің қажеті жоқ.

Ұсынылған операциялар тізбегі іске асырылған модельдің логикалық және есептеу құрылымын көрсетеді және міндеттемелерді қалыптастыру мен тексерудің дұрыстығын қамтамасыз етеді. Процедуралардың сипаттамалары бағдарламалық жасақтаманы икемдеуге және оның тиімділігін эксперименттік түрде бағалауға мүмкіндік береді.

Алгоритмді бағдарламалық қамтамасыз ету.

Ұсынылған теориялық модельді практикалық іске асыру мақсатында міндеттемелерді қалыптастыру және тексеру алгоритмдерінің жұмыс жасауын қамтамасыз ететін арнайы бағдарламалық құралды әзірлеу қажеттілігі туындады. Осыған байланысты сипатталған схемаға сәйкес негізгі криптографиялық процедураларды жүзеге асыратын VCNPSS v1.0 бағдарламалық кешені әзірленді. VCNPSS v1. 0 бағдарламалық кешені келесі негізгі компоненттерді қамтитын модульдік архитектураға ие:

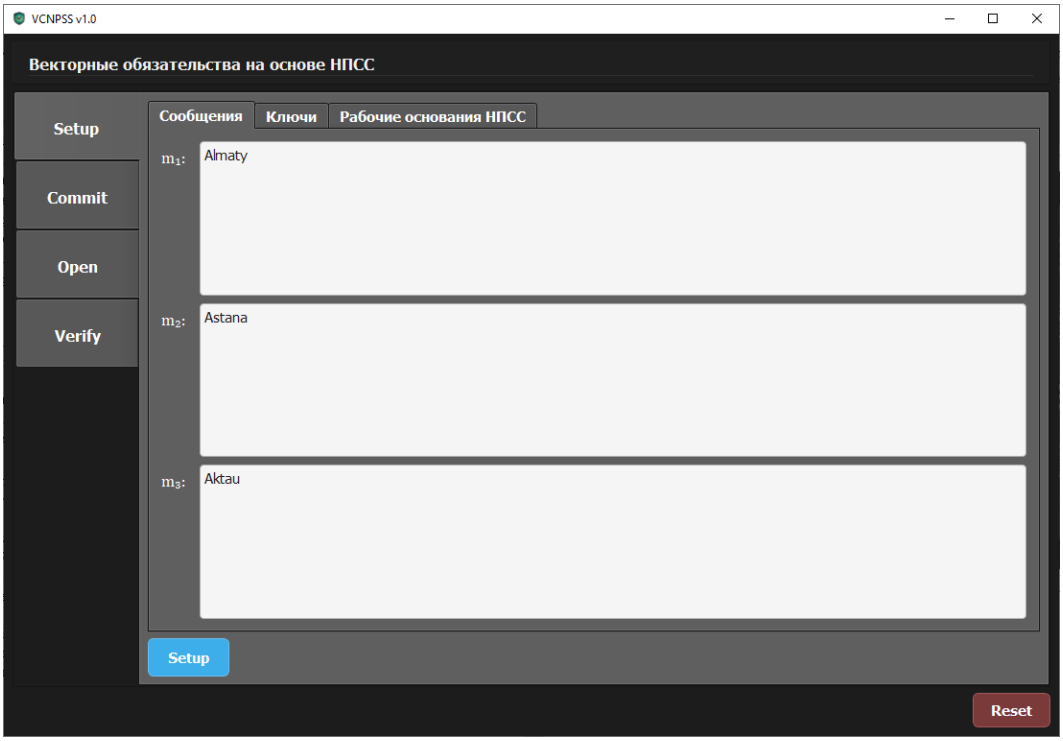
- Бастапқы параметрлерді генерациялайтын модуль,
- Хэштеу модулі,
- Криптографиялық есептеулер модулі,
- Пайдаланушы интерфейсі модулі.

Аталған VCNPSS v1.0 бағдарламалық кешені C++ бағдарламалау тілінде QT 5.15.18 нұсқасының фреймворкі және 6.3.0 нұсқасындағы GMP кітапханасының (GNU Multiple Precision Arithmetic Library) қолдауымен, сондай-ақ 11.6.0 нұсқасындағы NTL математикалық кітапханасының (Number Theory Library) көмегімен жүзеге асырылады.

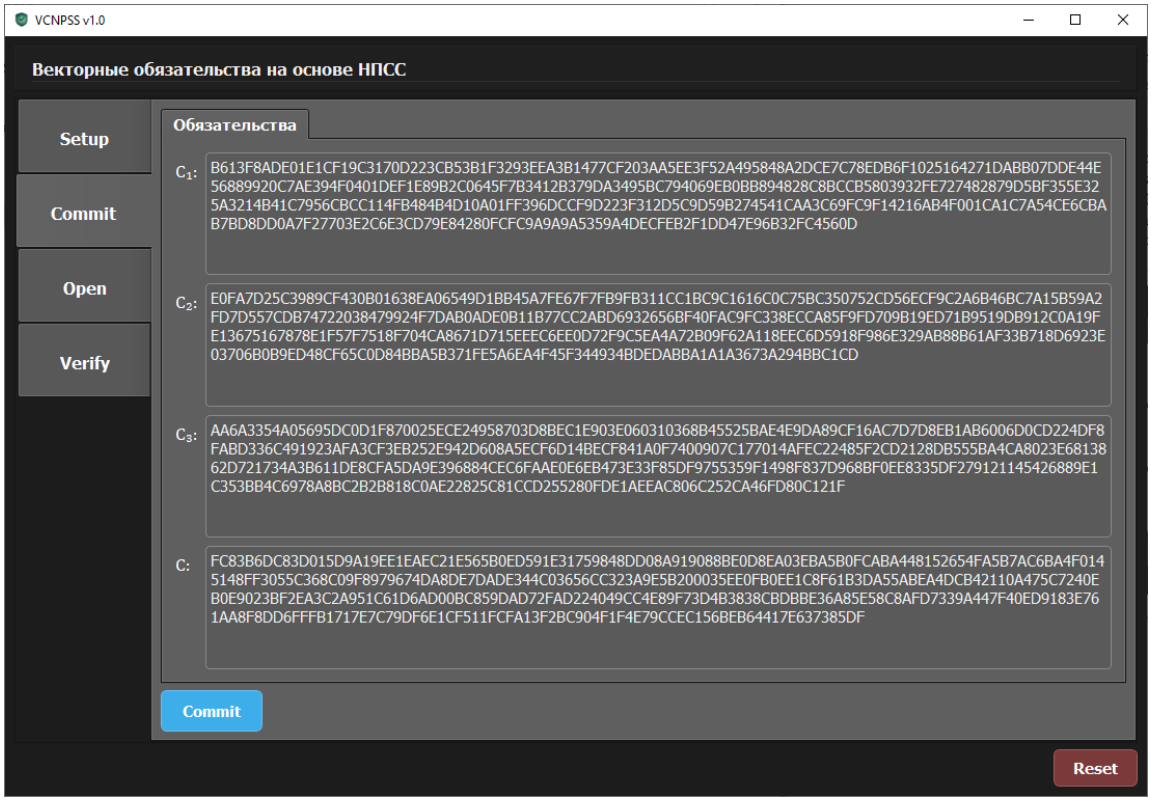
Төменде VCNPSS v1.0 бағдарламалық жасақтамасының негізгі кезеңдерін бейнелейтін пайдаланушы интерфейсінің мысалдары келтірілмейтін көпмүшеліктердің дәрежесі 512 болған жағдай бойынша келтірілген (Суреттер 2-5).

Бағдарламалық жасақтамада сандар теориясы мен алгебра саласында есептеулер жүргізуге арналған 11.6.0 нұсқасындағы NTL (Number Theory Library) кітапханасы қолданылды. Кітапхана ақырлы өрістерде үлкен бүтін сандар және полиномдармен жұмыс істеуге кең мүмкіндік береді, бұл GF(2) арифметикасын және қытайдың қалдықтар теоремасын қолдану үшін қажетті операцияларды жүзеге асыруға мүмкіндік берді.

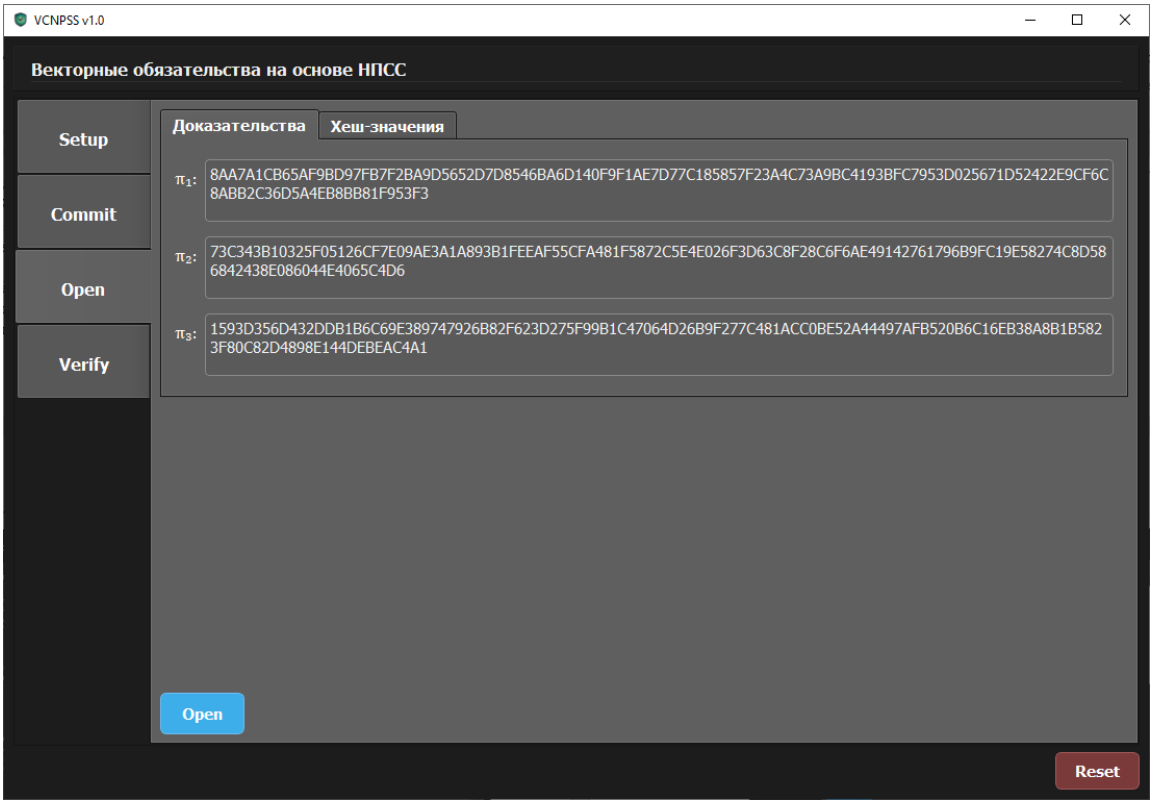
Өнімділікті арттыру үшін NTL кітапханасы тиімді дәлдік арифметикасын қамтамасыз ететін GMP кітапханасының (GNU Multiple Precision Arithmetic Library) қолдауымен жиналды. Бұл байламды пайдалану модульдік есептеу операцияларын жеделдетуге және жоғары дәрежелі полиномдармен жұмыс істеудің дұрыстығын қамтамасыз етуге мүмкіндік береді.



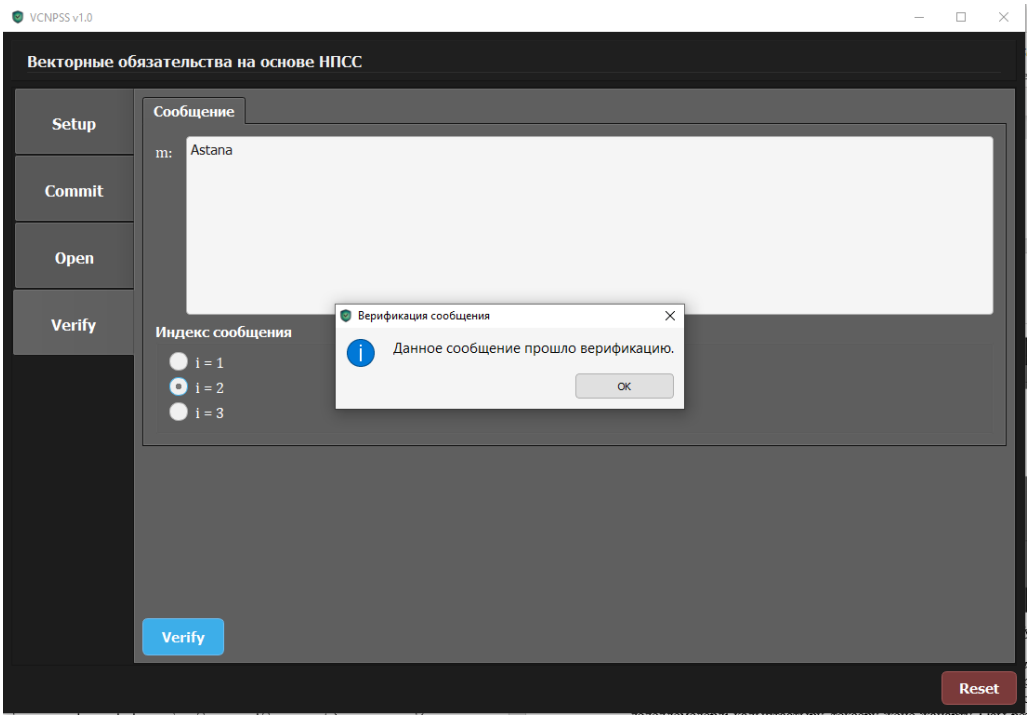
Сурет 2 – VCNPSS v1.0 бағдарламалық жасақтамасының негізгі терезесі (Setup кезеңі)



Сурет 3 – Генерацияланған криптографиялық міндеттемелерді бейнелеу (Commit кезеңі)



Сурет 4 – Криптографиялық дәлелдемелердің хабарламалардың міндеттемелеріне қатыстылығы бар екендігін бейнелеу (Open кезеңі)



Сурет 5 – Сәтті тексерілген хабарлама (Verify кезеңі)

Алгоритмнің есептеу тиімділігін теориялық тұрғыдан бағалау.

Әзірленген схеманың есептеу тиімділігін бағалау алгоритмдік кезеңдердің есептеу күрделілігін талдау негізінде жүргізілді. Яғни, кілттерді жасау, міндеттемелерді және

дәлелдемелерді қалыптастыру, тексеру және жаңарту. Осы ретте полиномдық арифметика операцияларының күрделілігіне және ҚҚТ қолдана отырып міндеттемені қайта құруға баса назар аударылады [10].

Есептеу күрделіліктері:

1. Дәлелдемелерді қалыптастыру кезеңінде.

Әрбір m_i , $i = 1, \dots, k$ хабарламасы үшін $H(m_i)$ хэш функциясын есептеу операциялары және g_i кілтімен XOR операциясы орындалады. Хэш кодтың белгіленген ұзындығы $n = 512$ болған жағдайда бір дәлелдемені қалыптастырудың күрделілігі $O(n)$, ал ағаштың барлық k түйіндері үшін $O(kn)$ болады.

2. Міндеттемені есептеу кезеңінде.

Ең көп ресурстарды қажет ететін кезең $C = \left(\sum_{i=1}^{k} \pi_i \, P_i P_i^{-1}\right) mod P$ полиномдық міндеттемені есептеу болып табылады. Мұнда, $O(k \cdot n^2)$ операцияны қажет ететін модульдердің көбейтіндісін есептеу, P_i модульдерді есептеу, КЕА әдісімен $O(n^2)$ есептеу қиындықтағы кері элементтерді табу, модульдік қосулар және модульдік салыстырулар төмендету сияқты есептеулер жүргізіледі. Ақырында, міндеттемені қалыптастырудың қорытынды асимптотикалық күрделілігі $O(kn^2)$ болып бағаланды.

3. Верификация кезеңінде.

Тексеру процедурасы қалдықты есептеуді, хэштеуді және XOR операциясын және мәндерді салыстыруды қамтиды. Бір хабарламаны тексерудің қиындығы $O(n^2)$.

4. Қытайдың қалдықтар теоремасын пайдалану.

Қытайдың қалдықтар теоремасын пайдалану P модулі бойынша есептеулерді p_i модульдері бойынша бір-біріне тәуелсіз операциялар жиынтығымен ауыстыруға мүмкіндік береді. Бұл есептің ыдырауын және параллельді іске асыру мүмкіндігін қамтамасыз етеді. Сол себепті бұл тәсіл алгоритмнің практикалық орындалу уақытын дәрежесі жоғары бір модуль бойынша тікелей есептеулермен салыстырғанда азайтады.

Кесте-1-де ҚҚТ негізделген полиномдық міндеттемелер схемасы мен классикалық KZG схемасының салыстырмалы талдауы келтірілген [11, 12]. Бұл кестеде міндеттемені қалыптастыру және тексеру кезеңдеріндегі дәлелдеме мөлшері және есептеу күрделілігі, сондай-ақ олардың қауіпсіздік қасиеттері сияқты параметрлер қарастырылады.

Салыстырмалы талдау үшін классикалық KZG схемасының таңдалуы ұсынылған әдістің мазмұнымен және құрылымымен тікелей байланысты. Ұсынылған тәсіл полиномдық міндеттемелерге негізделген болғандықтан, салыстыру біртекті криптографиялық модельдер шеңберінде жүргізілді. Осыған байланысты, ұсынылған схема үшін KZG міндеттемелерімен салыстыру есептеу тиімділігін, міндеттемелерді қалыптастыру және тексеру процестерінің күрделілігін тікелей және әдіснамалық жағынан дұрыс бағалауға мүмкіндік береді.

Кесте 1 – KZG полиноимальдық схемасымен салыстырмалы талдау

Параметрлер	Ұсынылған схема	KZG
Негізгі есептеулер типі	Полиномдық арифметика, CRT бойынша реконструкция	Эллиптикалық қисықтардағы және pairing есептеулер
Криптографиялық конструкция түрі	Полиномдық міндеттеме	Полиномдық міндеттеме
Дәлелдеме мөлшері	n дәрежелі бір π_i полиномы	G_1 группасындағы бір элемент

Міндеттемені қалыптастырудың қиындығы	полиномдармен жұмыс - $O(k \cdot n^2)$	Эллиптикалық қисықтардағы көбейту $O(d)$
Верификация күрделілігі	полиномдармен жұмыс - $O(n^2)$	Эллиптикалық қисықтардағы көбейту $O(log\ d)$
Өнімділіктің арту мүмкіндігі	k бойынша сызықты	Полином дәрежесі d -ға тәуелді
Негізгі күрделі операциялар	полиномдарды көбейту, кеңейтілген Евклид алгоритмі	Scalar multiplication, bilinear pairing
Бағдарламалық жүзеге асыру күрделілігі	Орташа	Жоғары
Аппараттық тәуелділік	Өте төмен (обычная арифметика)	жоғары (Эллиптикалық қисықтардағы және pairing есептеулер)
Постквантық беріктілік	иә	жоқ

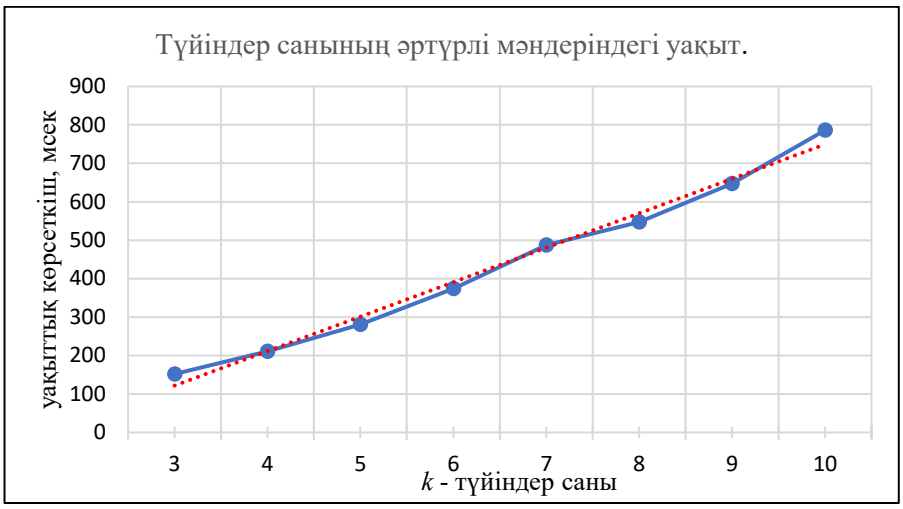
Салыстырмалы талдау көрсеткендей, ұсынылған схеманың есептеу моделі негізінен модулярлық арифметика операцияларына және ҚҚТ негізінде жүргізуге негізделген, ал KZG схемасы ресурстарды көп қажет ететін эллиптикалық қисықтар мен бисызықты бейнелеулер операцияларын қолданады. Эллиптикалық қисық операциялары жақсы оңтайландырылғанымен, олар арнайы криптографиялық примитивтерді қажет етеді. Ұсынылған схемада есептеу күрделілігі негізінен полиномдардың дәрежесімен және түйіндерінің саны *k*-мен анықталады, бұл есептеу үдерісінің үлкен көлемдегі деректерге бейімделуін қамтамасыз етеді. Сонымен қатар, KZG-ден үлкен айырмашылығы, ұсынылған схема постквантық беріктілікке ие.

Тиімділікті эксперименттік бағалау.

Эксперименттік бағалау алгоритмнің ең көп ресурстарды қажет ететін кезеңі болып табылатын C міндеттемесін қалыптастыру процедурасы үшін жүргізілді. Өлшеулер ҚҚТ қолдана отырып, n қауіпсіздік параметрінің әр түрлі мәндері және k түйіндерінің саны үшін орындалды.

Бағдарламалық жасақтама ерікті дәлдік арифметиканы қолдау үшін GMP кітапханасын қолданды. Бірақ бұл кітапхананың қорытынды уақыт сипаттамаларына әсері елеулі емес екендігін айта кету керек. Полиномдық арифметика операциялары және ҚҚТ бойынша міндеттемені қайта құру есептеу күрделілігінің негізгі үлесі болып табылады. Осылайша, алынған уақыттық көрсеткіштері төмен деңгейлі оңтайландыру ерекшеліктерін емес, ұсынылған схеманың алгоритмдік қасиеттерін көрсетеді.

Қауіпсіздік параметрінің бекітілген мәні $n = 512$ болғанда, k түйіндерінің көбеюі міндеттеменің қалыптасу уақытының сызықтық өсуіне әкеледі. Бұл тәуелділік ҚҚТ бойынша қайта құру алгоритмінің құрылымымен түсіндіріледі, онда міндеттеме $\pi_i P_i P_i^{-1}$ түріндегі k қосылғышының суммасы ретінде есептеледі. Әрбір қосымша түйін полиномдарды көбейту амалдарының жиынтығын орындауды, содан кейін $P(x)$ модулі бойынша қалындылар сақинасына қосуды талап етеді, бұл арифметикалық амалдардың жалпы санының пропорционалды өсуіне әкеледі (Сурет 6).

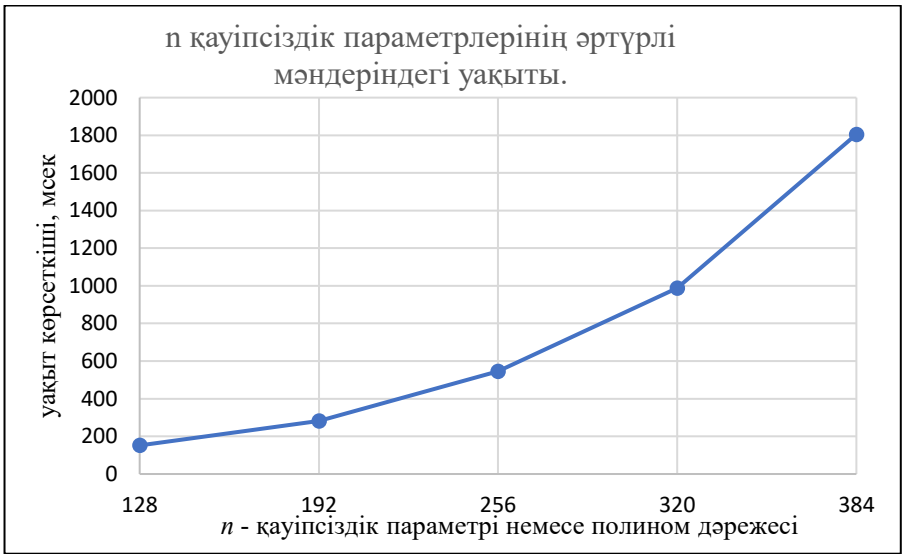


Сурет 6 – $n = 512$ үшін әртүрлі k мәндеріндегі уақыт динамикасы

Полиномдардың дәрежесі бекітілген n параметрі бойынша анықталатындықтан, әрбір жеке көбейту және модульге келтіру операцияларының есептеу күрделілігі шаманың реті бойынша тұрақты болып қалады. Бұл жағдайда, есептеу жүктемесінің өсуі негізінен k компоненттерінің санының артуымен анықталады (6-суреттегі қызыл сызықты қараңыз) және орындау уақытының түйіндер санына тәуелділігі сызықтық сипат құрайды.

Жүргізілген эксперименттік өлшеулер, қиындығы $O(n^2k)$ болатын теориялық бағалаумен практикалық нәтижелердің сәйкестігін растайды. Бұл криптографиялық беріктіліктің белгіленген деңгейінде алгоритмнің k параметрі бойынша ауқымын кеңейту мүмкіндігін көрсетеді. Құрылымдағы хабарламалар санының артуы есептеу шығындарының өсуіне әсер етеді.

Бекітілген $k = 3$ мәнінде n қауіпсіздік параметрінің жоғарылауы міндеттеменің қалыптасу уақытының сызықтық емес өсуіне әкеледі. Бұл әсерді n өскен сайын қолданылатын полиномдардың дәрежесі өсуімен, сондай-ақ арифметикалық операцияларға қатысатын коэффициенттердің разрядтарының артуымен түсіндіруге болады. Ол полиномдарды көбейтудің, модуль бойынша бөлу операцияларының және қалдықтарды есептеудің күрделілігіне тікелей әсер етеді (Сурет 7).



Сурет 7 – Бекітілген k=3 және әртүрлі n мәндеріндегі уақыт динамикасы

КЕА қолдана отырып, P_i^{-1} элементтерін табу кезеңі де жылдамдыққа ерекше әсер етеді. Полиномдар дәрежесінің жоғарылауымен алгоритмнің қайталану саны және аралық есептеу көлемі артады, бұл есептеу шығындарының квадраттық өсуіне әкеледі. ҚҚТ бойынша міндеттемені қайта құру операциясының санын арттыра түседі, өйткені $P(x)$ қосу және одан кейінгі модулі бойынша келтіру жоғары дәрежелі полиномдар үшін орындалады. Осылайша, қауіпсіздік параметрінің өсуі міндеттемені қалыптастырудың барлық негізгі кезеңдеріне кешенді әсер етеді, бұл орындалу уақытының ұлғаюының байқалған сызықтық емес динамикасын түсіндіреді.

Алынған нәтижелерде түйіндердің саны тұрақты болған жағдайда, күрделілігі $O(n^2)$ реттік теориялық бағамен сәйкес келеді (7-суретті қараңыз), сондай-ақ графигі параболалық түрмен сипатталады. Сонымен бірге, алгоритмнің ауқымын кеңейту мүмкіндігін растайды және қауіпсіздік параметрі n және түйіндерінің саны k сияқты криптографиялық параметрлердің жоғарылауымен есептеу шығындарының өсуін көрсетеді.

Бұл жұмыста хеш-функциясы ретінде LWH схемасы қолданылды. Аталған алгоритм криптографиялық губка (sponge) конструкциясына негізделген, бұл оның шығыс мәнінің ұзындығын икемді түрде өзгертуге мүмкіндік береді, яғни хеш-мәннің ұзындығы 128 битпен шектелмей 512 битке дейін ұлғайтылуы мүмкін. Сонымен қатар, ұсынылған цифрлық қолтаңба схемасы нақты бір хеш-функцияға байланбаған және коллизияға төзімді кез-келген криптографиялық хеш-функцияны қолдануға мүмкіндік береді. Осы тұрғыдан алғанда, SHA-3 және SHAKE сияқты стандартталған алгоритмдерді пайдалану ұсынылған модельге толықтай сәйкес келеді және оның қауіпсіздік деңгейін арттыруға мүмкіндік береді.

Қауіпсіздік моделі және криптографиялық қасиеттері.

Бұл бөлімде полиномдық міндеттемелер мен Verkle-ағаш құрылымына негізделген ұсынылған цифрлық қолтаңба схемасының негізгі қауіпсіздік қасиеттері келтіріледі. Айта кету керек, бұл жұмыстың мақсаты схеманың архитектурасын әзірлеу, оны бағдарламалық қамтамасыз ету және тиімділікті эксперименттік бағалау болып табылады. Осыған байланысты криптографиялық төзімділіктің қатаң дәлелдері толық көлемде әрі қарайғы зерттеулердің тақырыбы болып қала береді. Алайда, төменде қауіпсіздіктің негізгі қасиеттерінің ресми анықтамалары келтірілген және схемаға негізделген болжамдар талқыланады.

Байланыстыру қасиеті (Binding). Байланыстыру қасиеті қарсыластың бір міндеттемеге сәйкес келетін екі түрлі хабарламаны ала алмауын білдіреді.

Анықтама 1 (Байланыстыру). $Com(\cdot)$ міндеттемені қалыптастыру алгоритмі болсын. Егер кез-келген ықтимал $\mathcal{A}$ полиномдық алгоритм үшін $m \neq m'$ болатын және $Com(m) = Com(m')$ шартын қанағаттандыратын хабарламалар жұбын табу ықтималдығы өте аз болса, схема байланыстыру қасиетіне ие деп аталады.

Ұсынылған схемада байланыстыру қасиеті келесі факторлармен қамтамасыз етіледі:

- криптографиялық хэш функцияны қолдану;
- полинмдық міндеттемелердің құрылымдары;
- міндеттеменің жалған кездейсоқ қалыптасқан параметрлер жиынтығына тәуелділігі.

Осылайша, байланыстыру қасиетінің бұзылуы қолданылатын хэш функциядағы коллизияны табуға немесе полиномдық қайта құрудың дұрыстығын бұзуға дейін келтіреді.

Жасыру қасиеті (Hiding). Жасыру қасиеті қосымша параметрлерді білмей-ақ міндеттемеден хабарлама туралы ақпаратты алу мүмкін еместігін көрсетеді.

Анықтама 2 (Жасыру). Егер ұзындықтары бірдей m_0, m_1 екі хабарлама үшін олардың $Com(m_0)$ және $Com(m_1)$ міндеттемелері қарсылас үшін ажырата алмайтындай болса, онда схема жасыру қасиетіне ие деп аталады.

Ұсынылған схемада жасыру қасиеті келесі механизмдер арқылы қол жеткізіледі:

- міндеттемелерді қалыптастыру кезінде псевдокездейсоқ мәндерді қолдану;
- псевдокездейсоқтық қасиеттері бар хэш функцияны қолдану;
- қытайдың қалдық теоремасын қолдана отырып есептеулерді декомпозизиялау, бұл бастапқы деректерді тікелей қалпына келтіруді қиындатады.

Цифрлық қолтаңба схемаларына қойылатын стандартты талап – адаптивті хабарламаларды бұрмалауға төзімділік (Euf-CMA-Existential Unforgeability under Chosen Message Attack). Бұл жұмыста EUF-CMA моделіндегі тізбектің тұрақтылығының ресми дәлелі келтірілмеген. Дегенмен, схеманың құрылымы қолтаңбаны қолдан жасау мүмкіндігі келесі шарттарға байланысты деп болжанада: хэш функциясының коллизиясын табу; схеманың жасырын параметрлерін қалпына келтіру; міндеттемелердің қасиеттерін бұзу. EUF-CMA төзімділігінің толық ресми дәлелі жеке теориялық талдауды қажет етеді және әрі қарай зерттеу бағыты ретінде қарастырылады.

Қорытынды.

Жұмыста полиномдық құрылымдарды және Verkle ағашында қалдықтар туралы қытай теоремасын қолдануға негізделген полиномдық міндеттемелерді қалыптастыру мен тексеру схемасы ұсынылған. Әзірленген модель, құрылымның қалған элементтерін ашпай-ақ хабарламалардың тиістілігі туралы міндеттемелер мен дәлелдерді тиімді қалыптастыруға мүмкіндік береді. ҚҚТ қолдану арифметикалық амалдарды жеңілдетуге және деректерді өңдеу тиімділігін арттыруға ықпал ететін есептеулердің ыдырауын және полиномдық міндеттемені реконструкция мүмкіндігін қамтамасыз етеді.

Зерттеу барысында NTL математикалық кітапханасы мен GMP жоғары дәлдіктегі арифметика кітапханасын қолдана отырып, алгоритмнің бағдарламалық моделі енгізілді. Есептеу тиімділігіне жүргізілген талдау міндеттеменің қалыптасу уақыты n қауіпсіздік параметріне және k түйіндерінің санына байланысты екенін көрсетті. Эксперименттік нәтижелер күрделіліктің теориялық бағалауларын дәлелдеді. n белгілі бір мәнеге бекітілген кезде k жоғарылауы есептеу шығындарының сызықтық өсуіне әкеледі, ал n жоғарылауы полиномдар дәрежесінің өсуіне және модульдік арифметика операцияларының күрделенуіне байланысты жұмыс уақытының сызықтық емес өсуіне әкеледі.

KZG полиномдық міндеттемелерінің классикалық схемасымен жүргізілген салыстырмалы талдау, ұсынылған схеманың бірқатар ерекшеліктері бар екенін көрсетті. Эллиптикалық қисықтар мен билинарлы карталар бойынша операцияларға негізделген KZG-ден айырмашылығы, ұсынылған тәсіл полиномдық арифметика мен ҚҚТ бойынша реконструкцияны қолданады. Бұл алгоритм топтық криптографиялық операцияларды қолданбай құрастырылған (RSA немесе т.б. сияқты), сондықтан оның қауіпсіздігі кванттық компьютер шешетін есептерге тәуелді емес және схеманың постквантты беріктілігін қамтамасыз етеді.

Алынған нәтижелер криптографиялық берік және үлкен деректерді өңдеуге бейім аутентификациялау механизмдерін құру үшін қытайдың қалдықтар теоремасына негізделген полиномдық міндеттемелерді пайдалану перспективасын көрсетеді. Әзірленген схема постквантты цифрлық қолтаңбаларды және векторлық міндеттеме құрылымдарын пайдаланатын басқа криптографиялық хаттамаларды құру бойынша қосымша зерттеулерге негіз бола алады.

Зерттеу барысында ұсынылған әдістерді валидациялау мақсатында арнайы комьютерлік бағдарлама әзірленді, онымен https://cloud.mail.ru/public/G8D3/orePuvGmb сілтемесі арқылы танысуға болады. Бағдарламалық құрал n=512 дәрежелі келтірілмейтін көпмүшеліктерге негізделген модельдің тиімді жүзеге асырылуын қамтамасыз етеді.

Алғыс.

Зерттеу жұмыстары ҚР ҒЖБМ Ақпараттық және есептеу технологиялары институтында AP23488112 «Verkle ағашы негізінде кванттық төзімді цифрлық қолтаңба схемасын құру және зерттеу» жобасы аясында орындалды.

Әдебиеттер тізімі

1. Ducas, R., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seilor, G. & Stehle, D. (2021). CRYSTALS-Dilithium: Algorithm specification (Version 3.1); https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf.

2. Iavich, M., Gagnidze, A. & Iashvili, G. (2023). Verkle tree-based post-quantum digital signature: Algoritms and applications; CEUR Workshop Proceding, 3350, 1-12 https://ceur-ws.org/Vol-3550/paper13.pdf.

3. Khalfin, M. (2021). Chinese remainder theorem and cryptography, 45, https://michael-khalfin.github.io/michael-khalfin-cv/Chinese%20Remainder%20Theorem%20and%20Cryptography.pdf

4. Grossschadl, J. (2000). The Chinese remainder theorem and its application in a high-speed RSA crypto chip, In Proccedings of the 16th Annual Computer Security Applications Conference; New Orleans, LA, USA, 384-393, DOI: 10.1109/ACSAC.2000.898893.

5. Abid, R., Iwendi, C., Javed, A.R. et al. (2023). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication, Pers Ubiquit Comput; (27), 1405–1418, DOI: org/10.1007/s00779-021-01607-3.

6. Demir, E.D., Bilgin, B. & Onbasli, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algoritms; arXiv:2503.12952, DOI:10.48550/arXiv.2503.12952.

7. Algazy, K., Sakan, K. & Sawicki, D. (2025). A new digitial signature scheme based on the Verkle tree using the Chinese remainder theorem, In Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2025; (14009), 1-7, DOI: 10.1117/12.3099534.

8. Algazy, K., Sakan, K., Kapalova, N.A. & Alimzhan, Y.,Zh. (2025). A new approach to constructing vector commitments for the Verkle tree, Vestnik KazUTB; (3), 104-116, DOI: 10.58805/kazutb.v.3.28-928.

9. Sakan, K., Algazy, K., Kapalova, N. & Varennikov, A. (2025). Lightweight hash function design for the Internet of Things: Structure and SAT-based cryptanalysis, Algorithms; 18(9), 550, DOI: 10.3390/a18090550.

10. Omondi, A. & Premkumar, B. (2007). Residue number systems: Theory and implementation, Imperial College Press; 312, DOI: 10.1142/p523.

11. Kate, A., Zaverucha, G. & Goldberg, I. (2010). Constant-size commitments to polynomials and their applications, In ASIACRYPT 2010; (6477), 177-194, Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-17373-8_11.

12. Gabizon, A., Williamson, Z. & Ciobotaru, O. (2019). PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge, in IACR Cryptology ePrint; (2019), 953, https://ia.cr/2019/953.

ПРОВЕДЕНИЕ СРАВНИТЕЛЬНОГО АНАЛИЗА И ОЦЕНКИ ЭФФЕКТИВНОСТИ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ДЕРЕВА VERKLE

Аннотация. *В данной работе приводится оценка эффективности схемы цифровой подписи, разработанной на основе дерева Веркле с использованием непозиционной полиномиальной системы счисления. В предлагаемой схеме дерево Веркле позволяет сократить размер данных каждого узла за счёт выбора произвольного коэффициента ветвления и использования векторных обязательств. Непозиционная полиномиальная*

система счисления используется для аутентификации автора сообщения путём вычисления обязательств и соответствующих им доказательств. Для проверки подлинности сообщений используется разработанная хэш-функция, удовлетворяющая установленным требованиям безопасности. Был проведен анализ основных характеристик алгоритмов создания и проверки цифровой подписи, а также приведена оценка их сложности. Также представлен сравнительный анализ разработанной схемы цифровой подписи с цифровой подписью на основе криптографической схемы полиномиальных обязательств Kate-Zaverucha-Goldberg (KZG). Полученные результаты показывают, что обеспечение аутентификации и проверки подлинности сообщений с помощью цифровых подписей на основе дерева Веркле с использованием непозиционной полиномиальной системы счисления является перспективным направлением.

Ключевые слова: *дерево Verkle, векторное обязательство, полиномиальное обязательство, китайская теорема об остатках, цифровая подпись, аутентификация, верификация.*

PERFORMANCE EVALUATION AND COMPARATIVE ANALYSIS OF A DIGITAL SIGNATURE BASED ON A VERKLE TREE

Abstract. *This paper presents an experimental evaluation of the efficiency of the proposed digital signature based on a Verkle tree using the Chinese Remainder Theorem. A software implementation of the algorithms for key generation, signature formation, and verification has been developed. In the proposed scheme, the Verkle tree is used for compact representation of commitments, while the Chinese Remainder Theorem is applied to optimize modular computations and improve the computational efficiency of signing and verification operations. An analysis of the time characteristics of the algorithms was carried out, and complexity indicators were obtained. Experimental results were obtained on a fixed computing platform with multiple test runs to ensure statistical reliability. A comparative analysis was performed with a digital signature based on the classical polynomial commitment scheme Kate–Zaverucha–Goldberg (KZG) in terms of the main signature parameters and execution time. The obtained results demonstrate the potential of using the Verkle tree in combination with the Chinese Remainder Theorem for constructing compact and computationally efficient digital signatures.*

Keywords: *Verkle tree, vector commitment, polynomial commitment, Chinese Remainder Theorem, digital signature, authentication, verification.*

Авторлар туралы мәлімет

Сақан Қайрат Сақанұлы	PhD, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, E-mail: kairat_sks@mail.ru
Алғазы Күнболат Тілеуханұлы	PhD, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, E-mail: kunbolat@mail.ru
Варенников Андрей Владиславович	Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, инженер-программист, E-mail: avarennikov@gmail.com
Абишева Ақмарал Жолсеитовна	Абай атындағы Қазақ Ұлттық Педагогикалық университеті, Алматы, Қазақстан, аға оқытушы, E-mail: ak_maral@mail.ru

Сведение об авторах

Сакан Кайрат Саканулы	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kairat_sks@mail.ru
Алгазы Кунболат Тилеуханулы	PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан, E-mail: kunbolat@mail.ru
Варенников Андрей Владиславович	Институт информационных и вычислительных технологий, Алматы, Казахстан, инженер-программист, E-mail: avarennikov@gmail.com

Абишева Акмарал Жолсеитовна	Казахский национальный педагогический университет имени Абая, Алматы, Казахстан, старший преподаватель, E-mail: ak_maral@mail.ru

Information about the authors

Sakan Kairat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kairat_sks@mail.ru
Algazy Kunbolat	PhD, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, E-mail: kunbolat@mail.ru
VarennikovAndrey	Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, Software Engineer, E-mail: avarennikov@gmail.com
Abisheva Akmaral Zh.	Kazakh National Pedagogical University named after Abaya, Almaty, Kazakhstan, senior lecturer, E-mail: ak_maral@mail.ru