ҒТАХР 81.93.29
https://doi.org/10.56132/2791-3368-2026-2-66-75-85

К.Т. Алғазы[1], Е.Ж. Әлімжан[1,2], Қ.С. Сақан[1,2]
[1]Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан
[2]Farabi University, Алматы, Қазақстан
E-mail: ayerkebulan19@gmail.com

VERKLE-ҚҰРЫЛЫМДАРЫ ҮШІН ПОСТКВАНТТЫҚ ТОРЛЫ ВЕКТОРЛЫҚ МІНДЕТТЕМЕЛЕРДІ ҚҰРУ

Аңдатпа. Мақалада кванттық және кибернетикалық қауіптер жағдайында жұмыс істейтін әскери және арнайы мақсаттағы қорғалған таратылған ақпараттық жүйелер үшін деректердің аутентификациясының постквантық құрылымдарын құру мәселесі қарастырылады. Негізгі назар дәлелдеме құрылымдарының ықшамдылығын, локальды жаңартуды қолдауды және кванттық шабуылдарға төзімділікті қамтамасыз ететін торлы векторлық міндеттемелерге негізделген Verkle ағашын әзірлеуге бағытталған. Міндеттемелер және дәлелдеме модификацияларын ағашты толық қайта есептемей орындауға мүмкіндік беретін жаңартуларды локальды тарату әдісіне ерекше назар аударылады. Ұсынылған тәсіл деректерді жаңарту кезінде есептеу шығындарының төмендеуін қамтамасыз етеді және шектеулі есептеу ресурстары мен тұрақсыз байланыс арналары жағдайында таратылған ақпаратты сақтау жүйелерінің жұмыс істеу тиімділігін арттырады.

Түйінді сөздер: постквантық криптография, Verkle ағашы, торлы криптография, киберқауіпсіздік, әскери байланыс жүйелері.

Кіріспе.

Ақпараттық технологиялардың қарқынды даму заманында мемлекеттік әскери және арнайы күштік құрылымдар үшін ақпаратты қорғауды және оның қауіпсіздігін дамыту маңызды қадам болып табылады. Кванттық компьютерлердің пайда бола бастауына байланысты әскерлерді басқару үшін қолданатын заманауи ақпараттық жүйелер, қорғалған байланыс арналарын және таға да басқа маңызды инфоқұрылымдарды заманға сай дамыту өзекті болып отыр [1].

Осы уақытқа дейін қолданыста болып келген алгоритмдер негізінен үлкен сандарды факторизациялау және ақырлы кеңістікте дискретті логарифмдеу сияқты есептердің қиындығына сүйенеді. Бірақ ондай криптографиялық алгоритмдер Шор алгоритмдері сияқты кванттық алгоритмдерге осал болып табылады. Ал, бұл өз кезегінде ұлттық қауіпсіздік және қорғаныс саласында ақпараттық жүйелер арнасын пайдаланып

хабарлама алмасуға қауіп төндіреді. Сондықтан да, кванттық компьютерлер арқылы шабуылдарға да берік болып келетін постквантық алгоритмдерді дамыту маңызды болып отыр [2-4].

Қазіргі криптографияның негізгі мақсаттарының бірі ретінде таратылған ақпараттық жүйелердегі үлкен көлемді деректердің тұтастығы мен құпиялылығын қамтамасыз етуді атауға болады [5, 6]. Мұндай мәселені шешуде, соңғы кездері Verkle ағашын қолдану көп зерттеліп жүр. Verkle ағашы деректердің тиесілігін дәлелдеуде ықшамды жол ұсынады және ол Merkle ағашының жетілдірілген нұсқасы болып табылады [7-9].

Аталған құрылымның негізгі ерекшелігі – векторлық міндеттемелерді пайдалана отырып ағаштың бүкіл құрылымын ашпай-ақ элменттің ағашқа тиесілігін дәлелдей алады. Жоғары да аталғандай, қолданыстағы міндеттемелердің көбі болашақта беріктілікті қамтамасыз етпей қалу мүмкіндігі жоғар. Сол себепті, Verkle ағашына енгізуге тиімді векторлық міндеттемелердің жаңа жолдарын қарастыру қажеттілігі артуда [10, 11].

Осыған байланысты криптографиялық беріктілік, дәлелдемелердің ықшамдығы және есептеу өнімділігі арасындағы тепе-теңдікті қамтамасыз ететін векторлық міндеттемелердің тиімді торлы схемаларын әзірлеу өзекті ғылыми міндет болып табылады.

Деректер құрылымында аутентификациялау саласында бірқатар зерттеулер жүргізілуде. [12] жұмыста қарасытрылып отырған негізгі мақсаттары дәлелдеме көлемін кішірейту, элементтің құрылымға тиесілігін дәлелдеу және есептеу жылдамдығын арттыру. Ұзақ уақыт бойы блокчейн сияқты аутентификация құрылымдары Merkle ағаштарын қолданып келеді [6]. Уақыт өткен сайын ақпарат көлемі артып келеді, сондықтан дәлелдеме құрылымы да сызықты өсуге алып келеді. Бұл өз кезегінде, үлкен көлемдегі жүйелердің тиімділін төмендетеді [7].

[11] мақалада көпмүшелік міндеттемелер мен бисызықты бейнелеулерді қолданатын KZG міндеттемелер (Kate–Zaverucha–Goldberg commitments) пайдаланылады. Бұл схемеда да элементтің тиесілігі мен дәлелдеменің ықшам жолы ұсынылған. Бірақ бұл схема постквантық беріктілікті қамтамасыз етпейді. Кванттық компьютерлер қолданысқа енген кезде Шор алгоритміне қарсы тұра алмайды.

Материалдар мен тәсілдер.

Зеттеу жұмысында постквантық криптографияда қолданылатын торлық әдістер қолданылды. Негізгі назар торлық есептердің күрделілігіне аударылды. Торлық есептер қазіргі уақытта кванттық алгоритмдер арқылы шешілмейді деп есептеледі. Сол себепті торлық есептер ұзақ мерзімге криптографиялық қорғауды қажет ететін жүйелер үшін маңызды негіздердің бірі болып саналады.

Торлық әдістер мен торлық құрылымдарды қолданудың басты себебі – кванттық есептеу құралдары дамыған жағдайда да деректердің тұтастығы мен қауіпсіздігін қамтамасыз етуі. Әсіресе үлкен көлемдегі деректерді сақтау

жүйелерінде және аутентификация құрылымдарында классикалық криптографиялық әдістердің орнына постквантық тұрақтылығы бар тәсілдерді қолдану қажеттілігі артып бара жатыр.

Verkle ағаштарында әрбір түйін бірнеше көрші элементтерден тұратын вектор арқылы сипатталады. Осы вектордың мәндері міндеттеме құру кезінде қолданылады. Торлық әдістер мен құрылымдардағы міндеттеме сақина немесе модуль үстіндегі алгебралық құрылым арқылы беріледі. Мысалы, есептеу келесі сақинада жүргізілуі мүмкін:

$$R_q = Z_q[x]/(f(x)),$$

мұндағы, q – сақина модулі, ал $f(x)$ – n дәрежелі көпмүшелік. Сақина көпмүшеліктермен жұмыс істеуге және оларды модуль арқылы ықшам түрде көрсетуге мүмкіндік береді.

Міндеттеме құру кезінде ашық матрица, құпия вектор және қателік векторы пайдаланады. Жалпы түрде бұл байланыс төмендегі өрнекпен сипатталады:

$$C = A \cdot s + e(mod\ q),$$

мұндағы, A – ашық параметр ретінде алынатын матрица, s – коэффициенттердің жасырын сақталатын құпия векторы, ал e – қателік векторы. Қателік векторы міндеттемені тікелей ашып қоюдан қорғайды және торлық есептің күрделілігіне сүйенетін қауіпсіздік қасиетін күшейтеді.Зерттеуде математикалық модельдеу және салыстырмалы криптографиялық талдау қолданылды. Әзірленген схеманың тиімділігін бағалау үшін ол бисызықтық бейнелеуге негізделген дәстүрлі векторлық міндеттемелер мен дискретті логарифмдік есептеу күрделілігінің болжамы салыстырылды. Салыстыру критерийлері болып дәлелдемелер өлшемі, міндеттеме және тексеру операцияларының есептеу күрделілігі, тсымалданатын деректердің көлемі және кванттық шабуылдарға төзімділік деңгейі қарастырылды.

Нәтижелер мен талқылаулар.

Жұмыстың негізгі ғылыми жаңалығы Verkle ағашында постквантық міндеттемелерді локальды жаңарту әдісі болып табылады. Жұмыста бір тармақтың өзгеруі түбір жолының әр деңгейіндегі бір позицияның локальды өзгеру тізбегі ретінде қарастырылады. Кейбір түйінде i позиция өзгерсін. Бұл позицияның ескі хэштелген мәні a_i. Жаңа хэштелген мән $a_i{}'$. Олардың арасындағы айырмашылық q модулі арқылы беріледі.

$$\Delta_i = a_i{}' - a_i \ (\mathrm{mod}\ q).$$

Түйіннің ескі міндеттемесі келесідей түрге ие:

$$C = Ar + a_1U_1 + \cdots + a_iU_i + \cdots + a_kU_k \pmod q.$$

i-ші позицияда өзгеріс енгеннен кейін жаңа міндеттемелер ескі a_iU_i үлестің орнына жаңа $a_i'U_i$ үлесі болу керек.

$$C' = Ar + a_1U_1 + \cdots + a_i'U_i + \cdots + a_kU_k \pmod q.$$

Жаңа және ескі міндеттеменің айырмашылығы тек бір позициядан ғана тәуелді:

$$C' - C = a_i'U_i - a_iU_i \pmod q.$$
$$C' - C = (a_i' - a_i)U_i \pmod q.$$

Δ_i ауыстырғаннан кейін біз локальды жаңарту формуласын аламыз.

$$C' = C + \Delta_iU_i \pmod q.$$

Бұл формула ұсынылған әдістің өзегі болып табылады. Ол бір позицияны өзгерткеннен кейін позициялық үлестердің барлық суммасын қайта есептеудің қажеті жоқ екенін көрсетеді. Ескі міндеттемені алып, Δ_iU_i бір түзету үлесін қосу жеткілікті.

Бұл тәсіл толық қайта есептеуден ерекшеленеді. Толық қайта есептеу түйіннің барлық позицияларын қайтадан өңдейді. Локальды жаңарту тек өзгертілген позицияны өңдейді.

Жаңартуды түбірге тарату.

Verkle ағашында жапырақтың өзгеруі тек сол жапырақтан түбірге дейінгі жолға әсер етеді. Ол жол келесідей болсын:

$$v_0, v_1, \ldots, v_d.$$

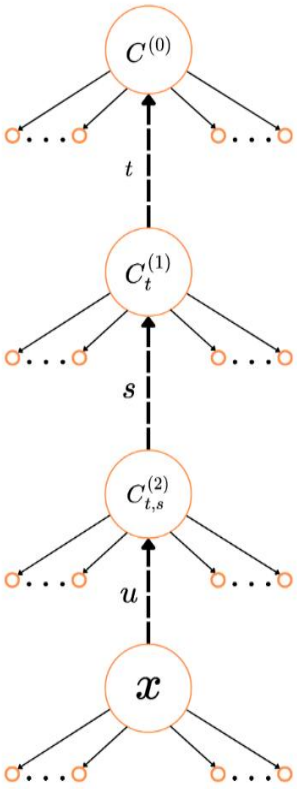
мұнда, v_0 түбір түйіні болып табылады. v_d түйіні өзгерген жапырақтарды қамтиды. Парақ мәнін өзгерткеннен кейін алдымен төменгі түйіннің тапсырмасы жаңартылады. Содан кейін осы түйіннің жаңа тапсырмасы аталық түйіндегі бір позицияның жаңа мәніне айналады.

Аталық түйін үшін жағдай өзгеріссіз қалады. Тек бір позиция өзгереді, сондықтан формула қайтадан қолданылады.

$$C_v' = C_v + \Delta_iU_i \pmod q.$$

Үдерісті түбірге дейін қайталайтын боламыз. Нәтижесінде жаңа түбірлік міндеттеме пайда болады. Ал, бұл жолдан тыс түйіндер өзгермейді. Сондықтан, олардың міндеттемелері қайта есептелмейді. Бұл принцип жаңартуды екі деңгейде локальды сипаттайды. Біріншіден, ол түйін аясында жасалады, яғни тек бір позиция ғана өзгереді. Екіншіден, ол ағаштың ішіндегі локальды өзгерісті білдіреді, мұнда тек бір жолдағы түйіндер ғана

өзгереді. Өзгертілген жапырақтан түбірге дейінгі жаңартудың локальды таралу схемасы сурет-1 де көрсетілген.



1 сурет – Verkle ағашындағы жаңартудың локальды таралу схемасы

Жолды дәлелдеуге әсері.

Локальды жаңарту әдісі жолды дәлелдеудің дұрыстығын сақтауы қажет. Ол үшін «куәгер» (witness) V_i-ді қарастыру маңызды. Егер ашалатын i-ші позиция өзгерсе, онда куәгерде $a_i R_i$ үлесі жоқ.

$$V_i = \sum_{j \neq i} a_j R_j + r \pmod{q}.$$

Сондықтан, бұл позиция үшін r куәгер өзгеріссіз қалуы мүмкін. Тексеру жаңа міндеттememен және жаңа $a_i{}'$ мәнімен орындалады $C' = AV_i + a_i{}'U_i \pmod{q}$. Егер басқа t позициясы өзгерсе және i позициясы ашылса, онда i позициясы үшін куәгер локальды түрде жаңартуға болады $V_i{}' = V_i + \Delta_t R_t \pmod{q}$. Бұл жаңарту сонымен қатар куәгерді толық қайта есептеуді қажет етпейді. Ол тек өзгертілген позиция айырмашылығын және қысқа R_t түпбейнені пайдаланады.

Сондықтан ұсынылған әдіс тек міндеттемені жаңартуын ғана қолдамайды. Ол сонымен қатар локальды ашылулардың тексерілуін сақтайды. Бұл path proof үшін маңызды. Verkle ағашындағы жол локальды ашылулар тізбегінен тұрады.

Локальды жаңартудың математикалық мысалы.

Демонстрациялық мысалды қарастырайық. Шағын параметрлер тек арифметиканы тексеру үшін қолданылады. Олар криптографиялық төзімділікке арналмаған.

Барлық есептеулер $q = 17$ модулі бойынша жүргізілсін және түйінде $k = 3$ позициясы бар.

Ашық $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ матрицасын және $r = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ жасырушы векторларын берілсін. Онда, $Ar = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 10 \\ 10 \end{pmatrix} \pmod{17}$.

Позициялардың ашық векторлары келесідей болады:

$$U_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \qquad U_2 = \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \qquad U_3 = \begin{pmatrix} 1 \\ 5 \end{pmatrix}.$$

Ескі хэштелген мәндері $a_1 = 3, \quad a_2 = 7, \quad a_3 = 4$ болсын. Онда ескі міндеттемелер $C = Ar + a_1U_1 + a_2U_2 + a_3U_3 \pmod{17}$ тең болады.

Сандарды орнына қойып, үлестерді есептейік.

$$C = \begin{pmatrix} 10 \\ 10 \end{pmatrix} + 3\begin{pmatrix} 2 \\ 1 \end{pmatrix} + 7\begin{pmatrix} 4 \\ 3 \end{pmatrix} + 4\begin{pmatrix} 1 \\ 5 \end{pmatrix} \pmod{17},$$

$$3U_1 = \begin{pmatrix} 6 \\ 3 \end{pmatrix}, 7U_2 = \begin{pmatrix} 28 \\ 21 \end{pmatrix}, 4U_3 = \begin{pmatrix} 4 \\ 20 \end{pmatrix}.$$

Сонда суммасы, $C = \begin{pmatrix} 10 \\ 10 \end{pmatrix} + \begin{pmatrix} 6 \\ 3 \end{pmatrix} + \begin{pmatrix} 28 \\ 21 \end{pmatrix} + \begin{pmatrix} 4 \\ 20 \end{pmatrix} = \begin{pmatrix} 48 \\ 54 \end{pmatrix} \pmod{17}$.

Модулге келтіргеннен кейін $C = \begin{pmatrix} 14 \\ 3 \end{pmatrix}$ аламыз. Енді екінші позицияны өзгертетін боламыз. Ескі мәні $a_2 = 7$ -ге тең, ал жаңа мәні $a_2{}' = 12$ -ге тең. Айырымдары, $\Delta_2 = a_2{}' - a_2 = 12 - 7 = 5 \pmod{17}$.

Ұсынылған әдіс бойынша жаңа міндеттеме локальды түрде есептеледі, $C' = C + \Delta_2 U_2 \pmod{17}$.

Сандарды орнына қоятын болсақ, $C' = \begin{pmatrix} 14 \\ 3 \end{pmatrix} + 5\begin{pmatrix} 4 \\ 3 \end{pmatrix} \pmod{17}$.

Түзету үлесін есептейік $5U_2 = \begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

Онда, $C' = \begin{pmatrix} 14 \\ 3 \end{pmatrix} + \begin{pmatrix} 20 \\ 15 \end{pmatrix} = \begin{pmatrix} 34 \\ 18 \end{pmatrix} \pmod{17}$ аламыз.

Модульге келтіргеннен кейін, $C' = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Жаңа міндеттеме түйінді толық қайта санамай-ақ алынды. Тек ескі міндеттеме және бір түзету үлесі қолданылды.

Мысалдан көрініп тұрғандай, ұсынылған әдістің айырмашылығы есептеу көлемінде болып тұр. Локальды жаңартусыз жағдайында, түйіндердің барлық міндеттемелері $a_1U_1, a_2{}'U_2, a_3U_3, \ldots, a_kU_k$ қайта есептелетін болса, ұсынылған әдісте тек Δ_iU_i есептеледі.

Үш позициялы кішкентай мысал үшін айырмашылық аз көрінеді. Тармақталу коэффициенті жоғары Verkle түйіні үшін бұл айырмашылық айтарлықтай болады. Егер түйінде $k = 256$ позиция болса, онда толық қайта есептеу барлық 256 үлесті қайта өңдеуді қажет етеді. Локальды жаңарту тек бір позицияны өңдеуді қажет етеді.

Ұсынылған тәсілдің ғылыми жаңалығы.

Зерттеудің ғылыми жаңалығы векторлық міндеттемелерге торлар теориясын қолдана отырып Verkle ағашы үшін жаңартуды локальды тарату әдісін кіргізу болып табылады. Басқа әдістерден тағы ерекшелігі, жұмыс динамикалық режимді қарастырады. Мұндай жағдайда бір жапырақтың мәнін өзгерту түбір жолындағы локальды жаңартулар тізбегіне айналады.

Әрбір жол түйінінде жаңа міндеттеме ескі міндеттемені пайдалана отырып келесі формула бойынша есептеледі:

$$C_v' = C_v + \Delta_i U_i \ (\mathrm{mod}\ q).$$

Ұсынылған әдіс түйіннің барлық позицияларын толық қайта санауды болдырмайды. Ол жаңа түбірлік міндеттеме мен ағаштың жаңартылған күйі арасындағы байланысты сақтайды. Ол сонымен қатар, локальды дәлелдемені ашу бөлігінің дұрыстығын көрсетеді.

Зерттеу қорытындылары Verkle ағашының постквантық құрылымын ықшамда дәлелдемелер мен локальды жаңартуды пайдалана отырып жасау мүмкіндігін көрсетеді. Құрылымның негізгі артықшылықтарының бірі – дискретті логарфм қиындығы мен бисызықты бейнелеулерді қолданатын криптографиялық примитивтерден бас тарту. Оның орнына заманауи, болашақта да беріктілікті қамтамасыз ететін әдістерді қолдану.

Ұсынылған схеманы деректерді аутентификациялаудың ең көп таралған құрылымдарымен салыстыру кесте 1-де келтірілген.

1 кесте – Аутентификациялау құрылымдарын салыстыру

Қасиеттер	Меркл ағашы	KZG негізіндегі Verkle ағашы	Қолданыстағы торлық векторлық міндеттеме	Ұсынылған схема
Постквантық беріктілік	Иә	Жоқ	Иә	Иә
Дәлелдеме ықшамдылығы	Төмен	Жоғары	Орташа	Жоғары
Сенімді инициализация қажеттілігі	Жоқ	Иә	Жоқ	Жоқ
Локальды жаңарту мүмкіндігі	Ішінара	Ішінара	Шектеулі	Толық
Verkle-құрылымымен үйлесімділігі	Жоқ	Иә	Шектеулі	Иә
Бисызықты бейнелеуді қолдану	Жоқ	Иә	Жоқ	Жоқ

Кестеден көрініп тұрғандай, Merkle ағашы да хэш функцияларды қолдану арқылы постквантық беріктілікті қамтамасыз еткенменде ақпарат көлемі немесе ағаштың биіктігі артқанда тиімсіз болып қалуы мүмкін. Сонымен бірге, локальды жаңарту мүмкіндігі де салыстырмалы түрде төмендеу. Кесте 2-де криптографиялық қасиеттері салыстырмалы түрде берілген.

2 кесте – Криптографиялық сипаттамаларды салыстыру

Сипаттамалар	KZG-негіздегі Verkle	Торлық векторлық схемалар	Ұсынылған схема
Қауіпсіздік негізі	Дискретті логарифм	Ring-LWE / LWE	Ring-LWE
Шора алгоритміне тұрақтылығы	Жоқ	Иә	Иә
Ықшамдылық	Жоғары	Орташа	Жоғары
Локальды жаңарту	Шектеулі	Ішінара	Толық
Постквантылық	Жоқ	Иә	Иә

Кесте 2-де келтірілген мәліметтерге қарайтын болсақ. Ұсынылған схеманың бірқатар артықшылықтарын көруге болады. Атап айтқанда, ықшамдылығы жоғары, локальды жаңартулары толық және постквантық қасиеттерге ие.

Болашақ жұмыстар немесе алдағы зерттеудің перспективалы бағыттарын атай кетейік:

- дәлелдеме өлшемдерін және ашық параметрлерді оңтайландыру;
- торға негізделген Verkle ағашын аппараттық іске асыру;
- нөлдік жарияланымдарды әзірлеу.

Қорытынды.

Жұмыста әскери және арнайы мақсаттағы таратылған қорғалған ақпараттық жүйелерде қолдануға бағытталған торлы векторлық міндеттемелерге негізделген Verkle ағашының постквантық құрылымы ұсынылған. KZG міндеттемелеріне және дискретті логарифмнің күрделілігін болжауға негізделген қолданыстағы Verkle конструкцияларынан айырмашылығы, ұсынылған тәсіл белгілі кванттық шабуылдарға төзімділікті қамтамасыз ететін Ring-LWE криптографиялық примитивтерін пайдаланады.

Зерттеудің практикалық маңыздылығы – әзірленген схеманы келесі құрылымдарда қолдану мүмкіндігіне байланыты:

- қорғалған әскери байланыс желілері;
- таратылған әскерлерді басқару жүйелері;
- маңызды объектілерді киберқорғау инфрақұрылымдары;

– қорғалған ведомствоаралық өзара іс-қимыл жүйелеріне;
– барлау ақпаратын сақтаудың таратылған жүйелерінің таралуы.

Ұсынылған тәсілді кванттық есептеу қатерлеріне және қазіргі заманғы криптоанализ құралдарына төзімділікті талап ететін перспективалы киберқорғаныс және қорғалған деректер алмасу жүйелерінде қолдануға болады.

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

1. Algazy K., Sakan K., Nyssanbayeva S., Lizunov O. Syrga2: Post-Quantum Hash-Based Signature Scheme // Computation. 2024. Vol. 12. P. 1–17. DOI: 10.3390/computation12060125.

2. Lyubashevsky V., Nguyen N. K. Advances in Cryptology – ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV // Advances in Cryptology – ASIACRYPT 2022. 2022. P. 95–125. DOI: 10.1007/978-3-031-22972-5_4.

3. Wee H., Wu D. J. Lattice-Based Functional Commitments: Fast Verification and Cryptanalysis // Advances in Cryptology – ASIACRYPT 2023. Singapore: Springer Nature, 2023. P. 1–41.

4. Cini V., Malavolta G., Nguyen N. K., Wee H. Polynomial Commitments from Lattices: Post-Quantum Security, Fast Verification and Transparent Setup // Advances in Cryptology – CRYPTO 2024. Cham: Springer, 2024. LNCS. Vol. 14929. DOI: 10.1007/978-3-031-68403-6_7.

5. Fenzi G., Moghaddas H., Nguyen N. K. Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency // Journal of Cryptology. 2024. Vol. 37. No. 31. P. 1–92. DOI: 10.1007/s00145-024-09511-8.

6. Kuznetsov O., Frontoni E., Kuznetsova K., Arnesano M. Optimizing Merkle Proof Size Through Path Length Analysis: A Probabilistic Framework for Efficient Blockchain State Verification // Future Internet. 2025. Vol. 17. No. 2. P. 1–20. DOI: 10.3390/fi17020072.

7. Kuznetsov O., Kanonik D., Rusnak A., Yezhov A., Domin O. Adaptive Restructuring of Merkle and Verkle Trees for Enhanced Blockchain Scalability // Internet of Things. 2024. Vol. 27. P. 1–34. DOI: 10.1016/j.iot.2024.101315.

8. Kuszmaul J. Verkle Trees. MIT PRIMES Research Papers. Cambridge, MA: Massachusetts Institute of Technology, 2019. 12 p. Available online: https://math.mit.edu/research/highschool/primes/materials/2018/Kuszmaul.pdf (accessed on 10 April 2026).

9. Kuszmaul J. Verkle Trees: Ver (y Short Mer)kle Trees. Presentation at PRIMES Conference, Cambridge, MA: Massachusetts Institute of Technology, 19 May 2019. 40 slides. Available online: https://math.mit.edu/research/highschool/primes/materials/2019/conf/12-5-Kuszmaul.pdf (accessed on 10 April 2026).

10. Catalano D., Fiore D. Vector Commitments and Their Applications // Public-Key Cryptography — PKC 2013. Berlin; Heidelberg: Springer, 2013. LNCS. Vol. 7778. P. 55–72. DOI: 10.1007/978-3-642-36362-7_5.

11. Kate A., Zaverucha G. M., Goldberg I. Constant-Size Commitments to Polynomials and Their Applications // Advances in Cryptology – ASIACRYPT 2010. Berlin; Heidelberg: Springer, 2010. LNCS. Vol. 6477. P. 177–194. DOI: 10.1007/978-3-642-17373-8_11.

12. Pathak V., Ruj S., van der Meyden R. Vector Commitment Design, Analysis, and Applications: A Survey // Cryptology ePrint Archive. Paper 2025/667. 2025. Available online.

Kunbolat Algazy, PhD, associate professor, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, kunbolat@mail.ru

Yerkebulan Alimzhan, doctoral student, Institute of Information and Computational Technologies CS MSHE RK, Farabi University, Almaty, Kazakhstan, ayerkebulan19@gmail.com

Kairat Sakan, PhD, Institute of Information and Computational Technologies CS MSHE RK, Farabi University, Almaty, Kazakhstan, kunbolat@mail.ru

CONSTRUCTION OF LATTICE-BASED VECTOR COMMITMENTS FOR VERKLE STRUCTURES

Abstract. This paper addresses the problem of constructing post-quantum authenticated data structures for secure distributed information systems operating under potential quantum and cyber threats. The primary focus is on the development of a Verkle tree based on lattice vector commitments, providing compact proof structures, support for local updates, and resistance to quantum attacks. Particular attention is given to the local update propagation mechanism, which enables modification of commitments and proofs without full recomputation of the tree. The proposed approach reduces computational overhead during data updates and improves the efficiency of distributed storage systems operating under limited computational resources and unstable communication channels. The proposed scheme can be applied in secure distributed storage systems, cyber defense infrastructures, and protected communication environments requiring post-quantum security guarantees.

Keywords: post-quantum cryptography, Verkle tree, lattice cryptography, Ring-LWE, cybersecurity, secure communication systems.

Күнболат Алғазы, PhD, ассоциированный профессор, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Казахстан, kunbolat@mail.ru

Еркебұлан Әлімжан, докторант, Institute of Information and Computational Technologies CS MSHE RK, Farabi University, Алматы, Казахстан, ayerkebulan19@gmail.com

Қайрат Сақан, PhD, Institute of Information and Computational Technologies CS MSHE RK, Farabi University, Алматы, Казахстан, kunbolat@mail.ru

ПОСТРОЕНИЕ РЕШЕТОЧНЫЕ ВЕКТОРНЫЕ КОММИТМЕНТЫ ДЛЯ VERKLE-СТРУКТУР

Аннотация. В статье рассматривается проблема построения постквантовых структур аутентификации данных для защищенных распределенных информационных систем военного и специального назначения, функционирующих в условиях потенциальных квантовых и кибернетических угроз. Основное внимание уделяется разработке Verkle-дерева на основе решеточных векторных коммитментов, обеспечивающего компактность доказательства-структур, поддержку локального обновления и устойчивость к квантовым атакам. Особое внимание уделено методу локального распространения обновлений, позволяющему выполнять модификацию обязательство и доказательства без полного пересчета дерева. Предложенный подход обеспечивает снижение вычислительных затрат при обновлении данных и повышает эффективность функционирования распределенных систем хранения информации в условиях ограниченных вычислительных ресурсов и нестабильных каналов связи.

Ключевые слова: постквантовая криптография, дерево Verkle, решетчатая криптография, кибербезопасность, военные системы связи.

Қабылданған күні: 02 маусым 2026 ж.
Рецензиядан өткен күні: 09 маусым 2026 ж.
Мақұлданған күні: 15 маусым 2026 ж.