ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№2
2026

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

2 (358)

APRIL – JUNE 2026

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).
Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.
Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*
Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

COMPUTER SCIENCE

МАЗМҰНЫ

КОМПЬЮТЕРЛІК ҒЫЛЫМДАР

СОДЕРЖАНИЕ

КОМПЬЮТЕРНЫЕ НАУКИ

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 2.
Namber 358 (2026). 67–86

https://doi.org/10.32014/2026.2518-1726.427

IRSTI 81.93.29
UDC 004.056

© Algazy K.[1], Alimzhan Y.[1,2,*], Sakan K.[1,2], Nyssanbayeva S.[1], 2026.
[1]Institute of information and computational technologies, Almaty, Kazakhstan;
[2] Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: ayerkebulan19@gmail.com

LATTICE-BASED VECTOR COMMITMENTS FOR VERKLE TREES

Algazy Kunbolat — PhD, associate professor, Institute of information and computational technologies, Almaty, Kazakhstan,
E-mail: kunbolat@mail.ru, ORCID ID: https://orcid.org/0000-0003-3670-2170;
Alimzhan Yerkebulan — PhD student at Al-Farabi Kazakh National University, Almaty, Kazakhstan,
E-mail: ayerkebulan19@gmail.com, ORCID ID: https://orcid.org/ 0009-0008-7600-9139;
Sakan Kairat — PhD, senior researcher, Institute of information and computational technologies, Almaty, Kazakhstan,
E-mail: kairat_sks@mail.ru, ORCID ID: https://orcid.org/0000-0002-6812-6000;
Nyssanbayeva Saule — doctor of technical sciences, professor, Institute of information and computational technologies, Almaty, Kazakhstan,
E-mail: sultasha1@mail.ru, ORCID ID: https://orcid.org/0000-0002-5835-4958.

Abstract. This paper presents a new lattice-based vector commitment scheme specifically optimized for Verkle trees and grounded in the hardness of the SIS problem. The main motivation is the development of compact and post-quantum secure cryptographic primitives suitable for scalable authenticated data structures used in modern blockchain systems and distributed ledgers. The proposed construction preserves the small proof and commitment sizes typical of classical vector commitments while ensuring resistance against quantum attacks and eliminating the need for a trusted setup. The paper provides a detailed description of the Setup, Commit, Open, and Verify algorithms, together with a formalized security model and clearly defined scheme parameters. Special attention is given to efficient encoding of polynomial coefficients into lattice space, principled parameter selection, and techniques for generating short witnesses with controlled norms, enabling a practical balance between security and computational efficiency. The construction is shown to support efficient multi-openings and batch verification, which are essential for high-arity Verkle tree paths and large-scale datasets. A comparative evaluation with classical commitment schemes such as KZG, IPA, and RSA is also presented, focusing on proof size, computational cost, and trusted setup

requirements. The results highlight the advantages of the lattice-based approach for long-lived distributed systems where long-term cryptographic security is critical. The proposed scheme demonstrates practical applicability and opens the way for integrating post-quantum vector commitments into scalable blockchain infrastructures.

Keywords: cryptography, vector commitments, Verkle trees, lattice, post-quantum cryptography

***Funding**. This work was supported the Science Committee of the Ministry of Science and Higer Education of the Republic of Kazakhstan (Grant No. fund this research AP23488112 - Development and study of a quantum-resistant digital signature scheme based on a Verkle tree)*

For citations: Algazy K., Alimzhan Y., Sakan K., Nyssanbayeva S. Lattice-based vector commitments for Verkle trees. Academic Scientific Journal of Computer Science, 2026. — No.2. – P. 67-86. DOI: https://doi.org/10.32014/2026.2518-1726.427

© Алғазы К.Т. [1], Әлімжан Е.Ж.[1,2,*], Сақан Қ.С.[1,2], Нысанбаева С.Е.[1], 2026.
[1]Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан;
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: ayerkebulan19@gmail.com

VERKLE АҒАШТАРЫНА АРНАЛҒАН ТОРЛЫҚ ВЕКТОРЛЫҚ МІНДЕТТЕМЕЛЕР

Алғазы Күнболат — PhD, қауымдастырылған профессор, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан,
E-mail: kunbolat@mail.ru, ORCID ID: https://orcid.org/0000-0003-3670-2170;
Әлімжан Еркебұлан — әл-Фараби атындағы Қазақ ұлттық университетінің PhD докторанты, Алматы, Қазақстан,
E-mail: ayerkebulan19@gmail.com, ORCID ID: https://orcid.org/ 0009-0008-7600-9139;
Сақан Қайрат — PhD, аға ғылыми қызметкер, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан,
E-mail: kairat_sks@mail.ru, ORCID ID: https://orcid.org/0000-0002-6812-6000;
Нысанбаева Сауле — техника ғылымдарының докторы, профессор, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан,
E-mail: sultasha1@mail.ru, ORCID ID: https://orcid.org/0000-0002-5835-4958.

Аннотация. Мақалада Verkle-ағаштарында қолдануға арнайы оңтайландырылған және SIS есептерінің күрделілігіне негізделген жаңа торлық векторлық міндеттеме схемасы ұсынылады. Зерттеудің негізгі мақсаты болып заманауи блокчейн жүйелері мен үлестірілген реестрлерде қолданылатын масштабталатын аутентификацияланған деректер құрылымдары үшін ықшам әрі постквanттық тұрақты криптографиялық примитивтерді құру болып табылады. Ұсынылған құрылым классикалық векторлық міндеттемелерге

тән дәлелдер мен міндеттемелердің шағын өлшемін сақтай отырып, кванттық шабуылдарға төзімділікті қамтамасыз етеді және trusted setup қажеттілігін жояды. Жұмыста Setup, Commit, Open және Verify алгоритмдері егжей-тегжейлі сипатталып, қауіпсіздік моделі формализацияланған және схема параметрлері анықталған. Сонымен қатар көпмүшелер коэффициенттерін торлық кеңістікке тиімді кодтау әдістері, модульдік параметрлерді таңдау принциптері және нормасы бақыланатын қысқа куәліктерді генерациялау тәсілдері қарастырылған, бұл қауіпсіздік пен есептеу тиімділігі арасындағы тепе-теңдікті қамтамасыз етеді. Ұсынылған құрылым тиімді көпашуларды және пакеттік тексеруді қолдайтыны көрсетілген, бұл жоғары тармақталуы бар Verkle-ағаштары үшін аса маңызды. Сонымен қатар KZG, IPA және RSA міндеттемелерімен салыстырмалы талдау жүргізіліп, дәлелдер өлшемі, есептеу шығындары және trusted setup талаптары бойынша бағаланған. Нәтижелер ұзақ мерзімді үлестірілген жүйелер үшін торлық тәсілдің артықшылықтарын көрсетеді және посткванттық векторлық міндеттемелерді масштабталатын блокчейн инфрақұрылымдарына енгізу мүмкіндігін ашады.

Түйін сөздер: криптография, векторлық міндеттемелер, Verkle-ағашы, тор, посткванттық криптография

© Алгазы К.Т. [1], Алимжан Е.Ж.[1,2,*], Сакан К.С. [1,2], Нысанбаева С.Е.[1], 2026.

[1]Институт информационных и вычислительных технологий, Алматы, Қазақстан;

[2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан.

E-mail: ayerkebulan19@gmail.com

РЕШЕТОЧНЫЕ ВЕКТОРНЫЕ ОБЯЗАТЕЛЬСТВА ДЛЯ VERKLE-ДЕРЕВЬЕВ

Алгазы Кунболат — PhD, ассоциированный профессор, Институт информационных и вычислительных технологий, Алматы, Казахстан,
E-mail: kunbolat@mail.ru, ORCID ID: https://orcid.org/0000-0003-3670-2170;
Алимжан Еркебулан — PhD докторант Казахского национального университета имени аль-Фараби, Алматы, Казахстан,
E-mail: ayerkebulan19@gmail.com, ORCID ID: https://orcid.org/ 0009-0008-7600-9139;
Сакан Кайрат — PhD, старший научный сотрудник, Институт информационных и вычислительных технологий, Алматы, Казахстан,
E-mail: kairat_sks@mail.ru, ORCID ID: https://orcid.org/0000-0002-6812-6000;
Нысанбаева Сауле — доктор технических наук, профессор, Институт информационных и вычислительных технологий, Алматы, Казахстан,
E-mail: sultasha1@mail.ru, ORCID ID: https://orcid.org/0000-0002-5835-4958.

Аннотация. *Актуальность.* В статье предлагается новая решеточная схема векторного обязательства, специально оптимизированная для использования в Verkle-деревьях и основанная на сложности задачи SIS.

Актуальность исследования обусловлена необходимостью построения компактных и постквантово-устойчивых криптографических примитивов для масштабируемых аутентифицированных структур данных, применяемых в современных блокчейн-системах и распределенных реестрах. *Цель.* Разработать решеточную схему векторного обязательства для Verkle-деревьев, обеспечивающую компактность доказательств, устойчивость к квантовым атакам и отсутствие необходимости доверенной инициализации. *Методы.* В работе описаны алгоритмы Setup, Commit, Open и Verify, формализована модель безопасности и определены основные параметры предложенной схемы. Особое внимание уделено эффективному кодированию коэффициентов многочленов в решеточное пространство, выбору модульных параметров и разработке методов генерации коротких свидетельств с контролируемой нормой. Такой подход позволяет достичь баланса между криптографической безопасностью и вычислительной эффективностью. *Результаты и выводы.* Предложенная конструкция сохраняет малый размер доказательств и обязательств, характерный для классических векторных обязательств, одновременно обеспечивая устойчивость к квантовым атакам и устраняя необходимость trusted setup. Показано, что схема поддерживает эффективные многооткрытия и пакетную верификацию, что особенно важно для Verkle-деревьев с высокой арностью и большими наборами данных. Проведено сравнительное исследование с классическими схемами обязательств KZG, IPA и RSA по критериям размера доказательств, вычислительных затрат и требований к trusted setup. Результаты демонстрируют преимущества решеточного подхода для долгоживущих распределенных систем, где критична долговременная криптографическая устойчивость. Предложенная схема обладает практической применимостью и открывает возможности для интеграции постквантовых векторных обязательств в масштабируемые блокчейн-инфраструктуры.

Ключевые слова: криптография, векторные обязательства, Verkle-деревья, решетки, постквантовая криптография, SIS, блокчейн, распределенные реестры

Кіріспе. Verkle ағаштары классикалық Меркл ағаштарының шектеулері мен кемшіліктерін шешуге бағытталған, аутентификацияланған деректер құрылымдарының заманауи криптографиялық конструкциясы болып табылады. Бұл құрылымның негізгі ерекшелігі ретінде ағаш түйіндерінде сақталатын мәндерді байланыстыру үшін векторлық және полиномиалдық міндеттемелерді қолданылатынын атауға болады, бұл дұрыстық дәлелдерін анағұрлым ықшам әрі тиімді түрде ұсынуға мүмкіндік береді. Мұндай тәсіл дәстүрлі Merkle-дәлелдерімен салыстырғанда тиесілілік дәлелдерінің көлемін едәуір қысқартып, оларды тексеру кезеңіндегі есептеу шығындарын азайтады. Нәтижесінде Verkle ағаштары жоғары масштабталғыштық пен үлкен көлемдегі деректер жүйелерінде қолдануға жарамдылықты көрсетеді. Бұл

қасиеттер оларды блокчейн-платформаларында, криптографиялық деректер құрылымдарында және цифрлық қолтаңба схемаларында, дәлелдердің ықшамдығы мен верификация тиімділігі аса маңызды болған жағдайларда, перспективалы құралға айналдырады (Kuznetsov et.al., 2025).

Векторлық міндеттемелер тұтас мәндер жиынын бекітуге және кейіннен барлық деректер құрылымын ашпай-ақ жекелеген элементтердің дұрыстығын дәлелдеуге мүмкіндік беретін іргелі криптографиялық примитив. Осы ерекшелігінің арқасында олар нөлдік жариялау дәлелдемелері хаттамаларында, үлестірілген тізілімдерде және жоғары тиімді деректерді тексеру жүйелерінде кеңінен қолданылады. Дәстүрлі түрде мұндай міндеттерде қолданылатын полиномиалдық міндеттемелер, көбіне Лагранж интерполяциясы сияқты интерполяциялық әдістерге немесе полиномның коэффициенттік көрінісіне негізделеді. Алайда мұндай әдістер әдетте міндеттемелер көлемінің едәуір ұлғаюымен және дәлелдерді генерациялау мен тексерудің жоғары есептеу күрделілігімен сипатталады, бұл олардың масштабталатын криптографиялық қолданбалардағы практикалық тиімділігін шектейді.

Verkle ағаштарында бинарлық хэш-міндеттемелердің орнына векторлық немесе полиномиалдық міндеттемелер қолданылады, бұл дәлелдемелердің өлшемін, тармақталу негізі бойынша логарифмге дейін қысқартуға мүмкіндік береді (Iavich et.al., 2023). Verkle ағаштарының негізгі элементі қысқа дұрыстық дәлелдерін қолданатын полиномиалдық міндеттеме схемасы (Polynomial Commitment, PC) саналады (Kuznetsov et.al., 2023). Практикада кең таралған полиномиалдық міндеттеме схемаларының көпшілігі эллиптикалық топтардағы дискретті логарифмдеу қиындығы (DLOG), CDH/DLP (Computational Diffie–Hellman, Discrete Logarithm Problem) болжамдарына немесе RSA-есептеріне негізделген. Ең танымал мысалдары ретінде Kate–Zaverucha–Goldberg (KZG) міндеттемелері және IPA (Infinitely-Parented Arrays) негізіндегі схемалар саналады (John et.al., 2019).

Хэш-функциялар кванттық (Гровердің квадраттық жылдамдату алгоритміне) тұрақты деп саналса да, дискретті логарифмдеуге, эллиптикалық қисықтарға және RSA (Rivest, Shamir and Adleman) негізделген криптографиялық схемалар кванттық модельде осал деп танылады (Algazy et.al., 2024). Бұл жағдай, векторлық міндеттемелерді, аутентификацияланған деректер құрылымдарын және ұзақ мерзімді блокчейн жүйелерінің күйлерін қоса алғанда, маңызды криптографиялық примитивтерді постквантық интеграциялау қажеттігін көрсетеді.

Кванттық есептеулер саласындағы прогреске байланысты АҚШ-тың Ұлттық стандарттар және технологиялар институты (ҰСТИ) постквантық криптографиялық алгоритмдерді стандарттау процесін бастады. 2022–2024 жылдары цифрлық қолтаңбалар мен кілт алмасу механизмдері үшін алғашқы стандарттар таңдалып, бекітілді.

Торлық міндеттемелер мен дәлелдер саласындағы белсенді зерттеулерге қарамастан, қолданыстағы конструкциялардың көпшілігі SNARK/IVC

сценарийлеріне бағытталған немесе дәлелдерінің сызықтық өлшемімен, үлкен тұрақтыларымен, тиімді жаңартылуды қолдамауымен сипатталады. Бұл оларды тармақталу коэффициенті жоғары Verkle ағаштарында қолдануға қолайсыз етеді (Lyubashevsky et.al., 2022).

Қысқа бүтін шешім (Short Integer Solution, SIS) және Қателермен оқыту (Learning With Errors, LWE) есептеріне негізделген торлық конструкциялар ҰСТИтарапынанпостквантықкриптографияныңеңсенімдікандидаттарының бірі ретінде қарастырылады, сондықтан олар болашақ Verkle ағаштарының табиғи негізі болып саналады.

Торлық векторлық міндеттемелерді Verkle ағашының құрылымына интеграциялау (Wee et.al., 2023):

1. Постквантық тұрақтылықты қамтамасыз етеді, яғни қауіпсіздік CDH/RSA емес, SIS/LWE есептеріне негізделеді.

2. KZG міндеттемелеріне қарағанда сенімді бастапқы инициализация қажеттілігін жояды.

3. Verkle ағаштарының векторлық табиғаты есебінен дәлелдердің ықшамдығын сақтайды.

4. Жаңа икемділік қасиеттерін береді, мысалы жаңартылуды қолдау.

Бұл жұмыста Verkle ағаштарында қолдануға бағытталған жаңа толық негіздегі векторлық міндеттеме схемасы ұсынылады. Зерттеудің негізгі мақсаттары мыналар:

– иерархиялық деректер құрылымдарына жарамды торлық векторлық міндеттеме схемасын әзірлеу;

– ұсынылған схеманы Verkle ағашының архитектурасына интеграциялау;

– конструкцияның дұрыстығын, қауіпсіздігін және постквантық тұрақтылығын талдау;

– міндеттемелердің, дәлелдердің өлшемі және есептеу шығындары бойынша CDH және RSA негізіндегі қолданыстағы міндеттемелермен салыстыру.

Әдеби шолу. Соңғы жылдары полиномиалдық және векторлық міндеттемелер Verkle-ағаштарын қоса алғанда, масштабталатын аутентификацияланған деректер құрылымдарын құрудағы негізгі криптографиялық примитивке айналды. Қолданыстағы жұмыстардың басым бөлігі дискретті логарифмдеуге және эллиптикалық қисықтарға негізделген схемаларға бағытталған. Олар жоғары тиімділікті қамтамасыз еткенімен, постквантық тұрақтылыққа ие емес және көбіне сенімді бастапқы инициализацияны талап етеді. Осы бөлімде Verkle-ағаштарына бейімделген торлық векторлық міндеттемелердің қолданыстағы тәсілдеріне сыни талдау жүргізіледі.

Көптеген қолданыстағы векторлық міндеттеме схемалары дискретті логарифмдеу қиындығы немесе билинейлік бейнелеулер сияқты криптографиялық болжамдарға сүйенеді, бұл есептеу ресурстары мен қауіпсіздік параметрлеріне қосымша талаптар қояды. Сонымен қатар,

бірқатар схемаларда дәлел өлшемі мен верификация құны ағаш түйіндерінің арлығы (арность) артқан сайын өседі.

Алғашқы зерттеулер стандартты криптографиялық болжамдарға, соның ішінде билинейлік топтардағы RSA және Diffи–Хеллманға негізделген векторлық міндеттемелер құруға бағытталды (Catalano et.al., 2013). Бұл жұмыстар ықшам міндеттемелер мен ашуларды алуға болатынын көрсетіп, деректерді аутентификациялау және жинақтағыштар үшін шешімдердің тиімділігін едәуір арттырды.

Кейінгі зерттеулер алгебралық құрылымдар мен билинейлік топтарға негізделген тиімді міндеттемелерді жасауға арналды. (Kate et.al., 2010) жұмысында тұрақты өлшемді дәлелдері бар полиномиалдық міндеттемелер ұсынылып, олар вектор элементтері бойынша полином интерполяциясы арқылы тиімді векторлық міндеттемелерді жүзеге асырады. Бұл конструкциялар дәлелдердің ықшамдығы мен тексерудің жоғары жылдамдығына байланысты тексерілетін есептеулер жүйелерінде және үлестірілген тізілімдерде кеңінен қолданылды.

Nutu et.al., (2025) мақаласында векторлық міндеттемелер мен олардың эволюциясына, соның ішінде торлық криптографиялық нұсқаларына кең шолу берілген. Шолу ауқымды болғанымен, полиномдық міндеттемелер схемасы (Polynomial Commitment Scheme, PCS) немесе Verkle тақырыптарына ғана бағытталмаған. Дегенмен, криптографиялық PCS эволюциясын және олардың қолданылуын оң тұрғыда талдап, міндеттемелердің жалпы контекстін түсінуге пайдалы.

Fenzi et.al., (2024) жұмысында торға негізделген полиномиалдық міндеттеме ұсынылады, ол дәлелдердің сығылған өлшемін және полином дәрежесіне байланысты тексеру уақытын қамтамасыз етеді, асимптотикалық және практикалық тиімділікке назар аударады. Бірегей көпмүшені конструктивті түрде алуға мүмкіндік беретін міндеттеме енгізіледі. Қауіпсіздік пен тиімділік нақты тұжырымдалғанымен, кейбір оңтайлы қасиеттерге қол жеткізу үшін кездейсоқ оракул немесе қосымша болжамдар қажет. Постквантты тұрақтылығына қарамастан, дәлел өлшемдері әзірге KZG сияқты эллиптикалық схемалардан үлкен.

Gini et.al., (2024) жұмысында авторлар ашық параметрлі (transparent setup) торлық тиімді шешімді ұсынады. Схема Module-SIS стандартты есебімен байланысты және Фиат–Шамир түрлендіруі арқылы кездейсоқ оракул моделінде интерактивті емес етуге болады. Қауіпсіздік деңгейі жоғары болғанымен, іске асыру күрделі және параметрлерді оңтайландыру бойынша қосымша зерттеулер қажет. Бұл жұмыс постквантты PCS схемаларының заманауи деңгейін көрсетеді.

Торлық векторлық міндеттемелер бойынша жұмыстарды екі класқа бөлуге болады: интерактивті емес конструкциялар және тор негізіндегі Bulletproofs протоколының бейімделген нұсқалары. Albercht et.al., (2024) жұмысында стандартты болжамдар негізінде полилогарифмдік дәлел өлшемі мен тексеру

уақыты бар extractable PCS жаңа класы ұсынылып, практикалық схемаларға жол ашатыны көрсетілген, алайда Verkle-ағаштары контекстінде қосымша бағалау қажет. Блокчейн саласында практикалық іске асырулар әзірге аз.

Nguyen et.al., (2024) жұмысында ұсынылған тәсілдің негізгі мақсаты, дәлел өлшемін азайту және практикалық жүйелердегі тексеру процедурасын жетілдіру. Ұсынылған схема шамамен 93 КБ көлеміндегі дәлелдерді генерациялайды және Verkle-ағаштарында қолдануға болатын PCS үшін идеялар ұсынады. Практикалық нәтижелері әсерлі болғанымен, қауіпсіздік тұрғысынан тереңірек талдау қажет.

Algazy et.al., (2024) жұмысында Verkle-ағаштарында CRT (Chinese Remainder Theorem) негізіндегі алгоритм қолданылып, үлестірілген жүйелер үшін шешімнің практикалық тиімділігі негізделеді. Жұмыс нақты қолданбалы мәселелерге бағытталғанымен, PCS қауіпсіздігінің іргелі аспектілерін терең қарастырмайды. (Iavich et.al., 2025) мақалаларында Verkle-құрылымдары мен торлық векторлық міндеттемелерді қолдана отырып, жадыны және қолтаңба өлшемін оңтайландыратын постквanттық цифрлық қолтаңба схемаларын құру зерттеледі, сондай-ақ кванттық шабуылдарға төзімділік пен тиімділікті арттыру үшін QRNG (Quantum Random Number Generator) интеграциясы ұсынылады.

Wang et.al., (2026) жұмысында блокчейндегі көптеген күйлерді (state) агрегатталған дәлелдер арқылы тексеру үшін Verkle-ағашы, Verkle-аккумулятор және KZG-полиномиалдық міндеттемелердің интеграциясы қарастырылады. Талдау нәтижесінде дәлелдер өлшемі мен тексеру жылдамдығы классикалық схемалардан жақсы екені көрсетілген.

Материалдар мен негізгі әдістер. *Векторлық міндеттемелер және олардың Verkle-ағаштарындағы рөлі*. Векторлық міндеттемелер (vector commitments, VC) жекелеген элементтерді кейін дәлелмен ашу мүмкіндігімен мәндер жиынын ықшам түрде бекітуге арналған криптографиялық примитивтер. VC негізгі қасиеттеріне дұрыстық (correctness), байланыстылық (binding), дәлелдердің қысқалығы және кейбір схемаларда жасырындық (hiding) жатады. Векторлық міндеттемелердің басты мақсаты ретінде деректер массивтерін тиімді аутентификациялау жатады.

Классикалық хэш-ағаштармен салыстырғанда, VC жоғары тармақталу кезінде кіші өлшемді дәлелдер алуға мүмкіндік береді. Дәл осы қасиет оларды масштабталатын блокчейн жүйелері мен күйді (state) сақтау тиімділігін арттыру үшін ұсынылған Verkle-ағаштарының негізгі элементіне айналдырады. Элементтің тиесілілігін дәлелдеу кезінде жапырақтан түбірге дейінгі жол бойындағы векторлардың тек қажетті позициялары ғана ашылады. Осылайша, Merkle-ағашындағыдай көршілес хэштердің толық жиынын берудің орнына, жекелеген индекстерді ашудың ықшам дәлелдері жеткілікті болады.

Verkle-ағаштары контекстінде векторлық міндеттемелер классикалық Merkle-ағаштарымен салыстырғанда асимптотикалық тұрғыдан ықшам

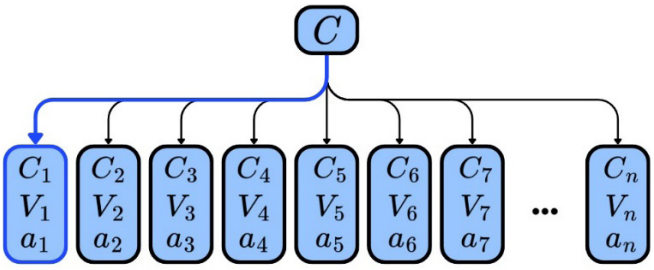
дәлелдер алуды қамтамасыз етеді және бір тармағының сұлбасы 1-суретте кескінделген. Verkle-құрылымдарында VC қолданудың негізгі идеялары:

– ағаш жапырақтары міндеттемелердің мәндерінен тұрады;

– ішкі түйіндер – еншілес түйіндер векторына жасалған міндеттемелер;

– векторлар көпмүше ретінде интерпретацияланады;

– элементтің ағашқа тиесілілігі бірнеше нүктедегі мәндерін ашу арқылы дәлелденеді.



Сурет 1 – Verkle ағашының бір тармағының сұлбасы.

Дәстүрлі Merkle-ағашында дәлел өлшемі шамамен $O(log\ n)$ және көптеген хэштерден тұрады. Ал Verkle-ағашында дәлел агрегатталып, қолданылатын міндеттеме схемасына байланысты тұрақтыға жақын немесе кіші коэффициентті логарифмдік өлшемде болуы мүмкін. Векторлық міндеттемелер мәндер жиынын бекітіп, кейін бүкіл құрылымды ашпай-ақ жекелеген компоненттердің дұрыстығын дәлелдеуге мүмкіндік береді. Бұл қасиет Verkle-ағаштарын үлестірілген тізілімдерде және ресурстары шектеулі хаттамаларда қолдану үшін ерекше тартымды етеді.

Торлар постквантық криптографияның негізі ретінде. Торлық криптография постквантық криптографияның ең перспективалы бағыттарының бірі болып саналады. Оның қауіпсіздігі келесі есептердің есептеу қиындығына негізделеді: SVP (Shortest Vector Problem), CVP (Closest Vector Problem), SIS (Short Integer Solution), LWE / Ring-LWE / Module-LWE. Алайда торлық міндеттемелерді, әсіресе Verkle-ағаштары контекстінде, векторлық формаға бейімдеу мәселесі әлі де жеткілікті зерттелмеген.

Анықтама 1 (Торлық векторлық міндеттеме).

Торлық векторлық міндеттеме – реттелген мәндер векторын бекітуге және оның жекелеген элементтерін кейін дәлелмен ашуға арналған $\Pi = (Setup, Commit, Open, Verify)$ криптографиялық схемасы. Ол келесі бөліктерден тұрады:

– $Setup\ (1^{\lambda}, n)$: Қауіпсіздік параметрі λ және вектордың максимал ұзындығы n бойынша $\Lambda \subset Z^m$ торымен немесе сәйкес Z_q^m модульдік кеңістігімен байланысты жария параметрлер pp генерацияланады. Параметрлерге міндеттемелер құру үшін қолданылатын кездейсоқ матрицалар немесе тор базистері кіреді.

– $Commit(pp, v)$: $v = (v_1, \dots, v_n), v_i \in Z_q$ векторы үшін $C = Com(v)$ міндеттемесін есептейді. Мысалы, $C = A\,v + e\,(mod\,q)$, мұнда A – жария етілетін (public) матрица, e – жасырындықты қамтамасыз ететін кіші кездейсоқ вектор.

– $Open(pp, v, i)$: i позициясындағы мәннің v_i екенін және оның C міндеттемесіне сәйкес келетінін дәлелдейтін π_i дәлелін құрады.

– $Verify(pp, C, v_i, \pi_i)$: ашудың дұрыстығын тексеріп, *accept* немесе *reject* нәтижесін қайтарады.

Нәтижелер. Бірінші кезекте, қолданылған белгілеулер мен параметрлерге тоқталайық. q – модулы ретінде жай сан таңдалады. $\mathbb{Z}_q$ арқылы q модулі бойынша қалдықтар сақинасын белгілейік. Векторлар мен матрицалар $\mathbb{Z}_q$ -де немесе $\mathbb{Z}$-те қарастырылып, кейін q модулі бойынша келтіріледі.

n, m, k (натурал) параметрлері беріледі, мұндағы k – коммиттелетін мәндер векторының ұзындығы. $A_i \in \mathbb{Z}_q^{n\times m}$ _ $i \in \{1, \dots, k\}$ позицияларына сәйкес келетін жария матрицалар, ал $U_i \in \mathbb{Z}_q^n$ – позициялардың жария вектор белгілері. Дәлелдің дұрыстығын бақылау үшін γ нормасына шек енгізіледі, яғни $\| V_i \| \leq \gamma$ шарты тексеріледі. Хеш-функция ретінде $H: \{0,1\}^* \to \mathbb{Z}_q$ немесе $H: \{0,1\}^* \to \{0,1\}^\lambda$ түріндегі криптографиялық тұрғыдан берік функцилар пайдаланылады.

Initialization (n,k). Инициализация кезеңінде (q, m) параметрлері бекітіледі, γ нормасына шектеулер таңдалады және H хеш-функциясы анықталады. m_i хабарламалары әрі қарай скалярлар түрінде қарастырылады:

$$a_i := H(m_i) \in \mathbb{Z}_q, i = 1, \dots, k.$$

$KeyGen(1^n)$. Әрбір $i \in \{1, \dots, k\}$ индексі үшін $A_i \in \mathbb{Z}_q^{n\times m}$ матрицасы таңдалады.

Сонымен қатар *trapdoor* деп аталатын T_i құпия ақпараты генерацияланады, ал $A_i x \equiv U (\mathrm{mod} q)$ түріндегі салыстырулар, кез-келген $u \in \mathbb{Z}_q^n$ үшін қысқа шешімдерді тиімді табуға мүмкіндік береді.

Одан кейін жария позициялық векторлар таңдалады:

$$U_1, \dots, U_k \in \mathbb{Z}_q^n.$$

Барлық $i \neq j$ индекс жұптары үшін қосымша қысқа элементтер анықталады:

$$R_{i,j} := SamplePre\left(T_i A_i U_j\right),$$

мұндағы, $SamplePre$ – қысқа түпбейнені таңдау процедурасы. Анықтама бойынша $A_i R_{i,j} \equiv U_j (mod\ q)$ және $\|R_{i,j}\|$ алдын-ала берілген параметрлермен шектеледі.

Схеманың жария параметрлері:

$$pp = (q, n, m, k, \{A_i\}_{i=1}^{k}, \{U_i\}_{i=1}^{k} = 1k, \gamma, H),$$

ал, коммиттердің құпия көмекші деректері $\{T_i\}$ немесе жүзеге асыруға байланысты $\{R_{i,j}\}_{i \neq j}$ жиыны ретінде берілуі мүмкін.

$\mathbf{Com_{pp}}(\mathbf{m_1}, \ldots, \mathbf{m_k})$. Барлық i үшін $a_i := H(m_i) \in \mathbb{Z}_q$ есептеледі. $(a_1, \ldots, a_k)$ векторына коммитмент келесідей анықталады:

$$C := \sum_{i=1}^{k} a_i \, U_i (\text{mod } q).$$

Алынған $C \in \mathbb{Z}_q^n$ векторы барлық позициялар үшін бірыңғай міндеттеме.

$\mathbf{Open_{pp}}(\mathbf{m_1}, \ldots, \mathbf{m_k})$. i-ші позицияны ашу қажет болған жағдайда, коммиттер барлық j үшін $a_j := H(m_j)$ есептейді. i позициясына дәлел алдын-ала дайындалған кері бейнелердің (preimage) тіркесімі ретінде анықталады:

$$V_i := \sum\nolimits_{j \neq i} a_j \, R_{i,j} (\text{mod } q).$$

Ашу (open) нәтижесі тексеруші a_i-ді өзі есептей ме соған байланысты (m_i, V_i) немесе (a_i, V_i) жұбы болып табылады.

$\mathbf{Ver_{pp}}(\mathbf{C}, \mathbf{i}, \mathbf{m_i}, \mathbf{V_i})$. Тексеруші $a_i := H(m_i)$ есептейді. Кейін екі шарт тексеріледі:

1. Дәлел нормасының шектеуі: $\| V_i \| \leq \gamma$.
2. Негізгі дұрыстық теңдігі: $C \equiv A_i V_i + a_i U_i (\text{mod } q)$.

Екі шарт та орындалса, ашу қабылданады және m_i хабарламасының C коммитментіне i-ші позицияға дұрыс тиесілі екендігі расталады.

Дұрыстықты негіздеу. Дұрыстық $R_{i,j}$ анықтамасынан туындайды. $j \neq i$ үшін шарт бойынша $A_i R_{i,j} \equiv U_j (\text{mod } q)$. Сонда,

$$A_i V_i + a_i U_i \equiv \sum_{j \neq i} a_j A_i R_{i,j} + a_i U_i \equiv \sum_{j \neq i} a_j U_j + a_i U_i = \sum_{j=1}^{k} a_j U_j \equiv C (\text{mod } q).$$

Демек, дұрыс құрылған V_i дәлелі әрқашан тексеруден өтеді.

Постквантық қауіпсіздікті 128 биттен төмен емес деңгейде қамтамасыз ету үшін келесі параметрлерді пайдалану ұсынылады:

- модуль: $q > 2^{23} \approx 8388608$;

- тор өлшемділігі: $n = 512$;
- бағандар саны: $m = 1024$.

Бұл параметрлер заманауи постквантты торлық криптографиялық схемалардың ұсынымдарына сәйкес келеді.

Ескерту. Толыққанды криптографиялық жүзеге асыруда дәлелдемелер trapdoor-параметрлерін және қысқа түпбейнелерді іріктеу процедураларын (мысалы, SamplePre тобы) пайдалану арқылы құрылады, сондай-ақ $\| V_i \| \leq \gamma$ шарты бақыланады. Келесі көрсетілетін мысалда, арифметиканы қолмен толық тексеруге мүмкіндік беру үшін квадратты A матрицасы және алдын ала дайындалған түпбейнелер қолданылады.

Сандық мысалға өтпестен бұрын, gadget-матрицаның, trapdoor-параметрлерінің және SamplePre процедурасының рөлін түсіндіру қажет. Бұл элементтер схеманың толық криптографиялық жүзеге асырылуына жатады. Олар ашу дәлелдемесінің қысқа болуын және оның q модулі бойынша дұрыс тексерілуін қамтамасыз етеді.

Gadget-матрица G құру үшін алдымен модуль q бойынша екілік разрядтар саны анықталады:

$$l = [log_2 q]$$

Бұл мән q модуліндегі кез-келген элементті екілік түрде көрсету үшін қажет болатын разрядтар санын береді. Осыдан кейін gadget-вектор енгізіледі:

$$g = (1,2,4, \dots, 2^{l-1}) \in Z_q^l.$$

Бұл вектор екілік жіктеу салмақтарынан тұрады. Яғни кез келген $t \in Z_q$ элементі осы салмақтар арқылы екілік түрде жазылады:

$$t = \sum_{s=0}^{l-1} b_s 2^s \ (mod\ q),$$

мұндағы $b_s \in \{0,1\}$. Сондықтан g векторы кейін G^{-1} операциясында қолданылады. Бұл операция вектор координаталарын екілік компоненттерге жіктейді.

n-өлшемді векторлармен жұмыс істеу үшін gadget-вектор g жеке координатаға ғана емес, барлық n координатаға қолданылады. Осы мақсатта бірлік матрица I_n алынады және gadget-матрица $G = I_n \otimes g$ құрылады. Нәтижесінде $G \in Z_q^{n \times nl}$ өлшемді матрица алынады. Бұл матрица блоктық құрылымға ие. Әрбір жолда gadget-вектор g тек бір координатаға сәйкес орналасады, ал қалған блоктар нөлдерден тұрады. Мысалы, $n = 3$ болған жағдайда G матрицасы мына түрде жазылады:

$$G = \begin{bmatrix} g & 0 & 0 \\ 0 & g & 0 \\ 0 & 0 & g \end{bmatrix}$$

Егер $g = (1,2,4, \ldots, 2^{l-1})$ болса, онда бұл матрица әрбір координатаны жеке екілік разрядтар арқылы қалпына келтіруге мүмкіндік береді. Сондықтан G матрицасы trapdoor-құрылымда негізгі техникалық құрал ретінде қолданылады. Ол A_i матрицасының жасырын құрылымын gadget-ұсынылым арқылы байланыстырады:

$$A_i \begin{bmatrix} T_i \\ I_{nl} \end{bmatrix} = G \ (mod\ q).$$

Осы байланыс кейін SamplePre процедурасында пайдаланылады. Атап айтқанда, $t_{i,j}$ векторы үшін алдымен оның екілік $b_{i,j} \leftarrow G^{-1}(t_{i,j})$ жіктелуі табылады. Содан кейін осы жіктеу арқылы қысқа түпбейне құрылады.

Әрбір $i \in \{1, \ldots, k\}$ позиция үшін $A_i \in Z_q^{n\times(m+nl)}$ ашық матрица құралады. Бұл матрица блоктық түрде беріледі, яғни $A_i = [\bar{A}_i \mid A_{i,2}]$, мұндағы $\bar{A}_i \in Z_q^{n\times m}$ – кездейсоқ компонент. Матрицаның екінші бөлігі кездейсоқ таңдалмайды. Ол G gadget-матрицасы және құпия trapdoor-матрица T_i арқылы анықталады:

$$A_{i,2} = G - \bar{A}_i\, T_i (mod\ q),$$

мұнда, $T_i \in Z_q^{m\times nl}$ құпия параметр болып табылады. Оны «қақпан» немесе trapdoor ретінде түсіндіруге болады. Егер, T_i белгісіз болса, онда $A_i R \equiv U(mod q)$ шартын қанағаттандыратын қысқа R векторын табу қиын есепке айналады. Мұндай есептің күрделілігі торлар теориясындағы қысқа шешімдерді табу есептерімен байланысты. Сондықтан A_i ашық матрицасы барлық қатысушыларға берілуі мүмкін. Ал құпия T_i матрицасы тек көмекші дәлелдемелерді құратын жақта сақталады.

Жоғарыда айтылған мәліметтерден A_i матрицасының арнайы түрде құрылғанын түсінуге болады. T_i арқылы A_i матрицасы G gadget-матрицасымен байланысады. Осы байланыс қысқа түпбейнені құру процедурасында қолданылады.

SamplePre процедурасы U_j векторының A_i матрицасына қатысты қысқа түпбейнесін құру үшін қолданылады. Индекстердің $i \neq j$ жұбы үшін ол келесідей жазылады:

$$R_{i,j} := SamplePre(T_i, A_i, U_j)$$

Бұл процедураның мақсаты $A_i R_{i,j} = U_j \ (mod\ q)$ шартын қанағаттандыратын $R_{i,j}$ векторын табу. Сонымен қатар $R_{i,j}$ қысқа болуы керек. Бұл шарт дәлелдеме нормасын тексеру үшін қажет, яғни $\| V_i \| \leq \gamma$.

Gadget-based нұсқада алдымен, $y_{i,j} \in Z^m$ қысқа вектор таңдалады. Содан кейін $t_{i,j} = U_j - \bar{A}_i\ y_{i,j} (mod\ q)$ қалдық вектор есептеледі. Бұл вектор U_j мәнінің қандай бөлігін gadget-блок арқылы алу қажет екенін көрсетеді. Кейін $b_{i,j} \leftarrow G^{-1}\ (t_{i,j})$ gadget decoding қолданылады. Мұнда, G^{-1} операциясы $t_{i,j}$ векторының әрбір координатасын екілік жіктеуге сәйкес келеді. Бұл жіктеу $(1,2,4, \dots, 2^{l-1})$ салмақтары бойынша орындалады.

Осыдан кейін қысқа түпбейне келесі формула бойынша анықталады:

$$R_{i,j} = \begin{bmatrix} y_{i,j} + T_i b_{i,j} \\ b_{i,j} \end{bmatrix} (mod\ q).$$

Бұл формуланың дұрыстылығын тікелей қою арқылы тексеруге болады.

$$A_i R_{i,j} = \left[\bar{A}_i \mid A_{i,2}\right] \begin{bmatrix} y_{i,j} + T_i b_{i,j} \\ b_{i,j} \end{bmatrix} = \bar{A}_i\ y_{i,j} + \bar{A}_i T_i b_{i,j} + (G - \bar{A}_i T_i) b_{i,j} (mod q)$$

мұнда, $\bar{A}_i T_i b_{i,j}$ бар мүшелер қысқарады. Сондықтан, $A_i R_{i,j} = \bar{A}_i y_{i,j}\ (mod\ q)$ өрнегі қалады. Ал $b_{i,j} = G^{-1}\ (t_{i,j})$ болғандықтан, $G b_{i,j} = t_{i,j} (mod\ q)$ теңдігі орындалады. $t_{i,\,j}$ анықтамасын ескерсек, $G b_{i,j} = U_j - \bar{A}_i\ y_{i,j} (mod\ q)$. Сонда, $A_i R_{i,j} = \bar{A}_i y_{i,j} + U_j - \bar{A}_i y_{i,j} = U_j (mod\ q)$.

Осылайша, $R_{i,j}$ векторы U_j векторының A_i матрицасына қатысты түпбейнесі екені дәлелденеді.

Толық схемада мұндай $R_{i,j}$ мәндері барлық $i \neq j$ жұптары үшін алдын ала құрылады. Кейін олар коммитменттің бір позициясын ашу кезінде қолданылады. Егер i-позицияны ашу қажет болса, онда дәлелдеме алдын ала дайындалған түпбейнелердің сызықтық комбинациясы ретінде құрылады:

$$V_i = \sum_{j \neq i} a_j\ R_{i,j} + r (mod\ q)$$

Осыдан кейін тексеруші тарап $C = A_i V_i + a_i U_i (mod\ q)$ теңдігін қолданады. Trapdoor-кезеңі құпия құрылымы бар матрицаны қалыптастырады. Ал SamplePre процедурасы осы құрылымды пайдаланып, қысқа түпбейнелерді алады.

Келесі сандық мысалда бұл процедура жеңілдетілген түрде көрсетіледі. Қолмен тексеруді жеңілдету үшін толық gadget-құрылымның орнына квадратты A матрицасы және алдын ала дайындалған түпбейнелер қолданылады. Бұл жеңілдету схеманың негізгі идеясын өзгертпейді, бірақ есептеулерді айқын көрсетеді.

Мысал. Торлы векторлық коммитменттің жұмыс істеу қағидатын көрсету үшін тәжірибелік мысал келтіріледі. Мақсатымыз коммитмент пен ашу дәлелін есептеу тәртібін көрнекі түрде көрсету, сондай-ақ верификация алгоритмінің негізінде жатқан теңдіктің тексерілуін көрсету.

Есептеулер $\mathbb{Z}_{101}$ −де жүргізіледі (барлық операциялар $q = 101$ модулінде орындалады).

$$A = \begin{pmatrix} 41 & 19 & 50 & 83 & 6 & 9 & 68 \\ 12 & 46 & 74 & 7 & 64 & 27 & 4 \\ 11 & 55 & 53 & 8 & 30 & 11 & 70 \\ 54 & 7 & 72 & 15 & 28 & 80 & 80 \\ 74 & 7 & 73 & 74 & 50 & 6 & 28 \\ 5 & 71 & 17 & 37 & 53 & 18 & 69 \\ 15 & 73 & 39 & 71 & 87 & 23 & 13 \end{pmatrix} (\mathrm{mod}101),$$

матрицасы және келесі ашық векторлары берілсін:

$$U_1 = (4,7,1,18,22,5,9), U_2 = (8,2,9,30,17,11,6), U_3 = (5,6,3,14,27,19,2),$$

Сонымен қатар, $a_i = H(m_i)$ мәндері де берілсін: $a_1 = 11, a_2 = 4,$ $a_3 = 13 \in \mathbb{Z}_{101}$. (a_1, a_2, a_3) үштігіне коммитменттер төмендегі комбинация арқылы анықталады:

$$C \equiv a_1U_1 + a_2U_2 + a_3U_3 (\mathrm{mod}101).$$

Координаталар бойынша көбейтінділерді есептеп, нәтижелерін 101 модулі бойынша келтіреміз:

$$a_1U_1 = 11 \cdot (4,7,1,18,22,5,9) = (44,77,11,198,242,55,99) \equiv (44,77,11,97,40,55,99),$$
$$a_2U_2 = 4 \cdot (8,2,9,30,17,11,6) = (32,8,36,120,68,44,24) \equiv (32,8,36,19,68,44,24),$$
$$a_3U_3 = 13 \cdot (5,6,3,14,27,19,2) = (65,78,39,182,351,247,26) \equiv (65,78,39,81,48,45,26).$$

Есептелген мәндерді қосатын болсақ,

$$C \equiv (44,77,11,97,40,55,99) + (32,8,36,19,68,44,24) + (65,78,39,81,48,45,26)$$
$$= (141,163,86,96,55,144,48) \equiv (40,62,86,96,55,43,48).$$

Нәтижесінде, $C \equiv (40,62,86,96,55,43,48)(\mathrm{mod}101)$.

1-позицияны ашу үшін дәлелдемені қалыптастыру.

Мысалда, $\mathrm{R}_2, \mathrm{R}_3$ түпбейнелерінің бар екені және олардың келесі салыстыру шарттарын қанағаттандыратыны болжанады:

$AR_2 \equiv U_2 (\mathrm{mod}101), AR_3 \equiv U_3 (\mathrm{mod}101)$, және оларды сандық тізбек

ретінде береміз, $R_2 = (93,78,20,24,66,20,100), R_3 = (74,87,100,9,51,63,15)$. 1-позицияның үшін *дәлелдемені* анықтап аламыз как $V_1 \equiv a_2R_2 + a_3R_3 (\mathrm{mod}101)$ және келесідей есептеулер жүргіземіз:

$$a_2R_2 = 4 \cdot (93,78,20,24,66,20,100) =$$
$$= (372,312,80,96,264,80,400) \equiv (69,9,80,96,62,80,97),$$
$$a_3R_3 = 13 \cdot (74,87,100,9,51,63,15) = (962,1131,1300,117,663,819,195)$$
$$\equiv (53,20,88,16,57,11,94).$$

Демек,

$$V_1 \equiv (69,9,80,96,62,80,97) + (53,20,88,16,57,11,94) =$$
$$= (122,29,168,112,119,91,191)$$
$$\equiv (21,29,67,11,18,91,90).$$

теңдігінің тексеру үшін есептеулер жүргіземіз.

Алдымен AV_1 есептеп аламыз. $V_1 = (21,29,67,11,18,91,90)$ болсын, онда A матрицасының жолдары бойынша келесі мәндерді есептеп аламыз:

$$(AV_1)_1 = 41 \cdot 21 + 19 \cdot 29 + 50 \cdot 67 + 83 \cdot 11 + 6 \cdot 18 + 9 \cdot 91 + 68 \cdot 90 = 12722 \equiv 97,$$
$$(AV_1)_2 = 12 \cdot 21 + 46 \cdot 29 + 74 \cdot 67 + 7 \cdot 11 + 64 \cdot 18 + 27 \cdot 91 + 4 \cdot 90 = 10590 \equiv 86,$$
$$(AV_1)_3 = 11 \cdot 21 + 55 \cdot 29 + 53 \cdot 67 + 8 \cdot 11 + 30 \cdot 18 + 11 \cdot 91 + 70 \cdot 90 = 13306 \equiv 75,$$
$$(AV_1)_4 = 54 \cdot 21 + 7 \cdot 29 + 72 \cdot 67 + 15 \cdot 11 + 28 \cdot 18 + 80 \cdot 91 + 80 \cdot 90 = 21310 \equiv 100,$$
$$(AV_1)_5 = 74 \cdot 21 + 7 \cdot 29 + 73 \cdot 67 + 74 \cdot 11 + 50 \cdot 18 + 6 \cdot 91 + 28 \cdot 90 = 11428 \equiv 15,$$
$$(AV_1)_6 = 5 \cdot 21 + 71 \cdot 29 + 17 \cdot 67 + 37 \cdot 11 + 53 \cdot 18 + 18 \cdot 91 + 69 \cdot 90 = 12512 \equiv 89,$$
$$(AV_1)_7 = 15 \cdot 21 + 73 \cdot 29 + 39 \cdot 67 + 71 \cdot 11 + 87 \cdot 18 + 23 \cdot 91 + 13 \cdot 90 = 10655$$
$$\equiv 50(mod101).$$

Бұдан, $AV_1 = (97,86,75,100,15,89,50)(\mathrm{mod}101)$

Әрі қарай, C алу кезінде есептелгендей,

$a_1U_1 = (44,77,11,97,40,55,99)(\mathrm{mod}101)$.

Алынған мәндерді қосатын болсақ,

$$AV_1 + a_1U_1 \equiv (97,86,75,100,15,89,50) + (44,77,11,97,40,55,99)$$
$$= (141,163,86,197,55,144,149) \equiv (40,62,86,96,55,43,48)(\mathrm{mod}101).$$

Демек,

$$C \equiv AV_1 + a_1U_1(\mathrm{mod}101),$$

яғни салыстырудың екі жағы тең.

Келтірілген мысал, есептелген C коммитментімен V_1 дәлелдеме тексеру, салыстыруды қанағаттандыратынын көрсетеді, яғни өрнектің екі бөлігі де q модулі бойынша сәйкес келеді. Ашуды жүзеге асыру процедурасының дұрыстығы расталады, ұсынылған мән бастапқы коммитментпен шынымен байланысты, әрі вектордың қалған компоненттері ашылмайды.

Талқылаулар. Классикалық Merkle-ағаштары қарапайымдылығы мен дәлелденген қауіпсіздігі арқасында блокчейн жүйелерінде кеңінен қолданылады. Алайда олардың бинарлық құрылымы қосылу дәлелінің өлшемінің логарифмдік түрде өсуіне әкеледі, бұл масштабтау кезінде маңызды мәселеге айналады. Verkle-ағаштарының олардан айырмашылығы, векторлық міндеттемелерді пайдаланады және бұл бір міндеттеме ішінде көптеген еншілес түйіндерді біріктіруге мүмкіндік береді. Соның нәтижесінде дәлелдердің өлшемі айтарлықтай кішірейеді. 1-кестеде Merkle және Verkle-ағаштарының салыстырмалы сипаттамалары келтірілген.

Кесте 1 – Merkle және Verkle ағаштарын салыстыру

Қасиеттер	Merkle ағашы	Verkle ағашы
Міндеттеме түрі	Хеш міндеттемелер	Векторлық немесе полиномдық міндеттемелер
Тармақталуы	Бинарлы	Жоғары (мысалы, 256)
Дәлелдеме өлшемі	$O(log_2 N)$ хеш	$O(log_b N)$ элементтер
Дәлелдемелерді біріктіру	Жоқ	Бар
Блокчейн жүйесінде қолдану	Қазір қолданылады	Болашақта ауыстру жоспарланады
Постквантық беріктілік	Қолданылған хешке байланысты	Міндеттеме схемасына байланысты

Ұсынылған Merkle және Verkle ағаштарының салыстырмасы аутентификацияланған деректер құрылымдары арасындағы негізгі архитектуралық және криптографиялық айырмашылықтарды көрсетеді. Осылайша, Verkle-ағаштары деректердің тексерілетіндігін сақтай отырып, анағұрлым жақсы масштабталуды қамтамасыз етеді.

Қолданыстағы векторлық міндеттеме схемаларын көрнекі талдау мақсатында 2-кестеде ең кең таралған тәсілдерге салыстырмалы зерттеу берілген. Олардың ішінде KZG-міндеттемелері, IPA схемалары, RSA-міндеттемелері, сондай-ақ ұсынылып отырған торлық векторлық міндеттеме схемасы қарастырылады. Салыстыру келесі негізгі критерийлер бойынша жүргізілді: криптографиялық негізі, постквантық тұрақтылығы, сенімді инициализацияның қажеттілігі, міндеттемелер мен дәлелдердің өлшемдері, верификацияның есептеу күрделілігі, дәлелдерді біріктіру мүмкіндігі және Verkle-ағаштары құрылымында қолданылуы.

Кесте 2 – Векторлық міндеттемелерді салыстыру

Критерийлер	KZG	IPA (Bulletproofs)	RSA-PC	Ұсынылған схеме
Криптографиялық негізі	CDH / DLOG	DLOG	RSA	SIS / LWE
Постквантық беріктілік	-	-	-	+
Сенімді инициализация (Trusted setup)	Қажет	Қажет емес	Қажет	Қажет емес
Міндеттеме өлшемі	$O(1)$	$O(n)$	$O(1)$	$O(n)$
Дәлелдеме өлшемі	$O(1)$	$O(\log\ n)$	$O(1)$	$O(\log\ n$
Верификация уақыты	$O(1)$	$O(\log\ n)$	$O(1)$	$O(\log\ n$
Дәлелдемені біріктіру	Иә	Иә	Шектелген	Иә
Verkle ағашына келуі	Иә	Иә	Ішінара	Иә
PQC үйлесімділігі	Жоқ	Жоқ	Жоқ	Иә

Кестеде көрсетілгендей, KZG-міндеттемелері өлшемі бойынша оңтайлы, бірақ постквантық болып табылмайды, IPA тәсілдері жақсы масштабталады, алайда есептеу жағынан ауыр, RSA-міндеттемелері икемділігі шектеулі және сенімді инициализацияны талап етеді. Ал торлық схема постквантық тұрақтылықты, trusted setup қажеттілігінің болмауын және Verkle-ағаштарымен үйлесімділікті бір мезгілде қамтамасыз ететін бірегей комбинацияны ұсынады.

Қорытынды. Алынған нәтижелер торлық векторлық міндеттемені Verkle-ағаштарының құрылымымен үйлесімді түрде құру мүмкіндігін және сенімді бастапқы инициализацияны талап етпейтінін растайды. SIS болжамдарын қолдану схеманың постквантық тұрақтылығын қамтамасыз етеді, бұл блокчейн жүйелері мен үлестірілген тізілімдер үшін шешуші маңызға ие қасиет.

Көпмүшенің коэффициенттерін торлық кеңістікке кодтау тәсілі полином арифметикасын модуль бойынша қысқа торлық векторлар арқылы тексерілетін қатынастармен тиімді байланыстыруға мүмкіндік береді. Нәтижесінде ашудың дәлелі куәгердің нормасын және қатынастың дұрыстығын тексеруге дейін төмендетіледі, бұл Verkle-ағаштарындағы верификация талаптарына жақсы сәйкес келеді.

Белгілі бір тармақталуы бар Verkle-түйінге (мысалы, 256 жапырақ) бір көпмүшені интеграциялау классикалық Merkle-ағаштарына қарағанда аутентификация деректерінің көлемін едәуір азайтуға мүмкіндік береді, сонымен қатар ашу дәлелдерінің логарифмдік күрделілігін сақтауға мүмкіндік береді. Міндеттеменің торлық сипаты ағаштағы жолдар үшін дәлелдерді біріктіру мүмкіндігін табиғи түрде қамтамасыз етеді, бұл бірнеше күй кілттерін тексеру кезінде әсіресе маңызды.

Жалпыға қолданылатын торлық міндеттемалар, яғни жалпы есептеулерге арналған немесе SNARK-қа ұқсас бағытталған шешімдерден айырмашылығы, ұсынылған конструкция Verkle-ағаштарының иерархиялық құрылымына оңтайландырылған. Бұл векторлардың тұрақты өлшемімен,

ашудың ықшамдалған үдерісімен және тиімді пакет бойынша верификация мүмкіндігімен көрініс табады. Осылайша алынған нәтижелер торлық векторлық міндеттемелердің тек теориялық тұрғыдан постквanттық тұрақты ғана емес, сонымен қатар масштабталатын деректер құрылымдарында практикалық түрде қолдануға жарамды екендігін көрсетеді.

References

Kuznetsov O, Frontoni E, Kuznetsova K, Arnesano M. (2025) Optimizing merkle proof size through path length analysis: a probabilistic framework for efficient blockchain state verification. Future Internet. – Vol.17(2). — No – 72. — P. 1-20 https://doi.org/10.3390/fi17020072 (in Eng.)

Iavich M.; Kuchukhidze T.; Bocu R. (2023) A Post-Quantum Digital Signature Using Verkle Trees and Lattices. Symmetry. – Vol. 15, 2165. – P.1-12 https://doi.org/10.3390/sym15122165 (in Eng.)

Kuznetsov O., Kanonik D., Rusnak A., Yezhov A. (2024) Domin O., Adaptive Restructuring of Merkle and Verkle Trees for Enhanced Blockchain Scalability. Internet of Things. – Vol. 27. – P.1-34 https://doi.org/10.1016/j.iot.2024.101315 (in Eng.)

John K. (2019) Verkle Trees. Available online: https://math.mit.edu/research/highschool/primes/materials/2018/Kuszmaul.pdf (accessed on 14 January 2023) (in Eng.)

Algazy K., Sakan K., Nyssanbayeva S. and Lizunov O. (2024) Syrga2: Post-Quantum Hash-Based Signature Scheme. Computation. – Vol. 12, 2165. – P.1-17. https://doi.org/10.3390/computation12060125 (in Eng.)

Lyubashevsky V., Nguyen N.K. (2022) 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. – P. 95 – 125. https://doi.org/10.1007/978-3-031-22972-5_4 (in Eng.)

Wee H., Wu D.J. (2023) Lattice-based functional commitments: fast verification and cryptanalysis, in Advances in Cryptology – ASIACRYPT 2023. Ed. by Jian Guo and Ron Steinfeld. (Springer Nature, Singapore, 2023). – P. 1–41. https://eprint.iacr.org/2024/028 (in Eng.)

Catalano D., Fiore D. (2013). Vector Commitments and Their Applications. In: Kurosawa, K., Hanaoka, G. (eds) Public-Key Cryptography – PKC 2013. PKC 2013. Lecture Notes in Computer Science. – Vol. 7778. Springer, Berlin, Heidelberg. – P. 55-72 https://doi.org/10.1007/978-3-642-36362-7_5 (in Eng.)

Kate A., Zaverucha G.M., Goldberg I. (2010) Constant-Size Commitments to Polynomials and Their Applications. In: Abe, M. (eds) Advances in Cryptology - ASIACRYPT 2010. ASIACRYPT 2010. Lecture Notes in Computer Science. – Vol 6477. Springer, Berlin, Heidelberg. – P. 177-194 https://doi.org/10.1007/978-3-642-17373-8_11 (in Eng.)

Nutu M., Akhalaia, G., Bocu R. Iavich M. (2025) An Extended Survey Concerning the Vector Commitments. Appled Science. – Vol.15(17). –P. 1-20 https://doi.org/10.3390/app15179510 (in Eng.)

Fenzi G., Moghaddas H., Nguyen, N.K. (2024) Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency. J Cryptol. – Vol.37. – No – 31. – P. 1-92. https://doi.org/10.1007/s00145-024-09511-8 (in Eng.)

Cini V., Malavolta, G. Nguyen, N.K., Wee H. (2024) Polynomial Commitments from Lattices: Post-quantum Security, Fast Verification and Transparent Setup. In: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. CRYPTO 2024. Lecture Notes in Computer Science. – Vol. 14929. Springer, Cham. https://doi.org/10.1007/978-3-031-68403-6_7 (in Eng.)

Albrecht M.R., Fenzi G., Lapiha O., Nguyen N.K. (2024) SLAP: Succinct Lattice-Based Polynomial Commitments from Standard Assumptions. In: Joye, M., Leander, G. (eds) Advances in Cryptology – EUROCRYPT 2024. EUROCRYPT 2024. Lecture Notes in Computer Science. – Vol. 14657. Springer, Cham. https://doi.org/10.1007/978-3-031-58754-2_4 (in Eng.)

Nguyen N.K., Seiler G. (2024) Greyhound: Fast Polynomial Commitments from Lattices. In: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. CRYPTO 2024. Lecture Notes in Computer Science. – Vol. 14929. Springer, Cham. https://doi.org/10.1007/978-3-031-68403-6_8 (in Eng.)

Algazy K., Sakan K., Nyssanbayeva S., Khompysh A. (2025) Polynomial Commitment in a Verkle Tree Based on a Non-Positional Polynomial Notation, CMC-Computers, Materials & Continua. – Vol.84. – No – 1. – P. 1581–1595 https://doi.org/10.32604/cmc.2025.065085 (in Eng.)

Iavich M., Kapalova N. (2025) Optimizing Post-Quantum Digital Signatures with Verkle Trees and Quantum Seed-Based Pseudo-Random Generators. Computers**. –** Vol. 14, 103. – P. 1-24. https://doi.org/10.3390/computers14030103 (in Eng.)

Wang S., Ma J., Huang H., Xie X. (2026) Verkle-Accumulator-Based Multiple State Verifiable and Updatable (VA-MSVU) scheme for blockchain. Journal of Network and Computer Applications. – Vol. – 245, 104392. – P. 1-17, https://doi.org/10.1016/j.jnca.2025.104392 (in Eng.)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Requirements for articles design for publication in the journal are available on the websites:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Managing Editor: *A.Shormakova*
Editors: *D.S. Alenov, T. Apendiev*
Computer layout: *G.D. Zhadyranova*

Signed for print: June 15, 2026
Format: 70×90 1/16. 26.5 printed sheets. Order No. 2.

«Central Asian Academic Research Center» LLP
Almaty, Shevchenko Street, 28