ҒТАМР 81.93.29 **https://doi.org/10.58805/kazutb.v.3.28-928**

VERKLE АҒАШЫНА ВЕКТОРЛЫҚ МІНДЕТТЕМЕЛЕРДІ ҚҰРУДЫҢ ЖАҢА ЖОЛЫ

[1]К.Т. Алғазы, [1,2]Қ.С. Сақан, [1,2]Н.А. Капалова, [1,2]Е.Ж. Алимжан
[1]Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан,
[2]Әл-Фараби атындағы қазақ ұлттық университеті, Алматы, Қазақстан
Корреспондент-автор: kairat_sks@mail.ru

Мақалада сандық қолтаңба схемасын құру үшін жаңа бағыт – Verkle ағашы мен қытайдың қалдықтар теоремасына негізделген векторлық міндеттемелерді қолдану ұсынылады. Verkle ағаштары – оңтайландырылған мерклдік құрылымдар, ал векторлық міндеттемелер ақпаратты тиімді әрі сенімді бекітуге мүмкіндік береді. Осы комбинация мүмкін болатын қауіптерге қарсы тұрақты, тиімді және ықшамды қолтаңба схемасын жасауға көмектеседі. Жұмыста векторлық міндеттемелер қытайдың қалдықтар теоремасына негізделген позициялы емес санау жүйелерді (ПЕСЖ) қолданып, қолтаңбаларды құрудың ғылыми негіздемесі мен мүмкіндіктері зерттеледі. ПЕСЖ – бұл теңдеулердің шешімдерін табуға бағытталған жүйелер, оларда айнымалылардың орналасу реті маңызды рөл атқармайды. Бұл схемалар арқылы қолтаңбалардың көлемін қысқарту және олардың дәлдігін тексеру тәсілі әзірленді. Бұл жүйелер, көбінесе, алгебралық құрылымдар мен модульдік арифметикаға негізделген. Сонымен қатар, хеш функцияларды пайдалану арқылы қолтаңбалардың қауіпсіздігін одан әрі арттырудың мүмкіндігі қарастырылады. Хеш функциялары криптографиялық жүйелерде деректердің тұтастығын, қауіпсіздігін және аутентификациялауды қамтамасыз ету үшін маңызды рөл атқаратын құрал ретінде пайдаланып келеді. Осы ғылыми зерттеуде позициялы емес санау жүйесін векторлық міндеттемелер үшін қолдану үлкен перспективаларға ие болатындығы көрсетілді. Бұл тәсіл міндеттемелердің тиімділігін арттырып қана қоймай, олардың қауіпсіздігін және қолдану аясын кеңейтеді. Бұл тәсіл Verkle ағаштарымен және басқа да криптографиялық құрылымдармен біріктіру арқылы постквантты қауіпсіздікке бейімделген криптографиялық шешімдер жасауға болады.

Түйін сөздер: Verkle ағашы, векторлық міндеттеме, цифрлы қолтаңба, аутентификация, верификация, криптография

НОВЫЙ ПОДХОД К ПОСТРОЕНИЮ ВЕКТОРНЫХ ОБЯЗАТЕЛЬСТВ ДЛЯ ДЕРЕВА VERKLE

[1]К.Т. Алгазы, [1,2]К.С. Сакан, [1,2]Н.А. Капалова, [1,2]Е.Ж. Алимжан
[1]Институт информационных и вычислительных технологий, Алматы, Қазақстан,
[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
email: kairat_sks@mail.ru

В статье предлагается новый подход к созданию схемы цифровой подписи с использованием векторных обязательств дерева Verkle, основаннах на китайской теореме об остатках. Деревья Verkle представляют собой оптимизированные структуры дерева Merkle, а векторные обязательства позволяют эффективно и надежно фиксировать информацию. Данная комбинация способствует разработке устойчивой, эффективной и компактной схемы подписи, защищенной от возможных угроз. В работе исследуются научные обоснования и возможности построения подписей с использованием векторных обязательств, основанных на непозиционной системе счисления (НПСС), применяющих китайскую теорему об остатках. НПСС – это системы, ориентированные на нахождение решений уравнений, в которых порядок расположения переменных не играет ключевой роли. Эти системы, как правило, базируются на алгебраических структурах и модульной арифметике. Разработанный метод позволяет сокращении размера подписей и проверки их точности. Кроме того, рассматривается возможность повышения безопасности подписей за счет использования хеш-функций. Хеш-функции играют важную роль в криптографических системах, обеспечивая целостность данных, безопасность и аутентификацию. В данном научном исследовании показано, что

применение НПСС для векторных обязательств обладает значительным потенциалом. Этот подход не только повышает эффективность обязательств, но и расширяет их сферу применения и уровень безопасности. Интеграция с деревьями Verkle и другими криптографическими структурами позволяет разрабатывать криптографические решения, адаптированные к постквантовой безопасности.

Ключевые слова: дерево Verkle, векторное обязательство, цифровая подпись, аутентификация, верификация, криптография

A NEW APPROACH TO CONSTRUCTING VECTOR COMMITMENTS FOR THE VERKLE TREE

[1]K.T. Algazy, [1,2]K.S. Sakan✉, [1,2]N.A. Kapalova, [1,2]Y.Zh. Alimzhan

[1]Institute of information and computational technologies, Almaty, Kazakhstan,
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,
email: kairat_sks@mail.ru

This paper proposes a novel approach to designing a digital signature scheme using vector commitments for the Verkle tree, based on the Chinese Remainder Theorem. Verkle trees are optimized structures derived from Merkle trees, while vector commitments enable efficient and secure information binding. This combination facilitates the development of a robust, efficient, and compact signature scheme resistant to potential threats. The study explores the theoretical foundations and feasibility of constructing signatures with vector commitments based on a non-positional notation (NPN) employing the Chinese Remainder Theorem. NPNs are systems designed for solving equations where the order of variables is not a determining factor. These systems are typically based on algebraic structures and modular arithmetic. The proposed method reduces signature size while ensuring their verification accuracy. Additionally, the paper examines the potential for enhancing signature security through the use of hash functions. Hash functions play a crucial role in cryptographic systems, ensuring data integrity, security, and authentication. This research demonstrates that applying NPNs to vector commitments holds significant potential. This approach not only improves the efficiency of commitments but also broadens their applicability and security level. Integration with Verkle trees and other cryptographic structures enables the development of cryptographic solutions adapted to post-quantum security.

Keywords: Verkle tree, vector commitment, digital signature, authentication, verification, cryptography

Кіріспе. Сандық қолтаңба схемалары қазіргі заманда қолданылып отырған криптографиялық құралдардың маңызды бір бөлігі болып табылады. Олардың көмегімен деректердің тұтастығын қамтамасыз етіп, пайдаланушылардың аутентификациясын орындайды және қауіпсіздік протоколдарының негізін құрайды. Қазіргі қолданыстағы қолтаңба алгоритмдері үлкен сандарды факторизациялау және элиптикалық қисықтың дискретті логарифимі сияқты есептердің қиындығына жүгінгенімен кванттық компьютерлер шабуылына қарсы тұра алмайды. Кванттық есептеулердің дамуы криптографиялық жүйелердің көпшілігіне қауіп төндіруде. Кванттық компьютерлердің күрделі математикалық есептеулерді орындауға қабілеттілігі, әсіресе асимметриялық криптографиялық алгоритмдердің қауіпсіздігіне әсер етеді. Мұндай технологиялар практикаға көптеп енген жағдайда RSA және ECC сияқты кеңінен қолданылатын криптографиялық жүйелерді алмастыруға тура келеді. Сондықтан, постквантық криптографияға арналған жаңа шешімдер әзірлеу қажеттілігі туындап отыр [1-3].

Постквантық криптографияға арналған схемалар классикалық компьютерлерде де, кванттық компьютерлерде де берік болатындай алгоритмдерді қамтиды. Мұндай заманауи алгоритмдер бірнеше бағытты қамтиды: торлық криптография, кодқа негізделген криптография, көпайнымалы полиномдарға негізделген криптография және хеш-функцияларға негізделген криптография жатады. Бұл мақалада соңғы бағытқа, яғни хеш-функциялар және век-

торлық міндеттемелер негізіндегі шешімдер зерттеледі. Аталған негіздегі постквантты алгоритмдер жоғары қауіпсіздік, қарапайымдылық және кванттық шабуылдарға төзімділік тұрғысынан үлкен артықшылықтарға ие. Сондықтан олар болашақта кеңінен қолданылады деп күтілуде, әсіресе цифрлық қолтаңба жүйелерінде, блокчейндерде және жалпы криптографиялық хаттамаларда [4-6].

2016 жылғы АҚШ-тың Ұлттық стандарттар және технологиялар институты жариялаған конкур нәтижесінде таңдалып алынған алгоритмнің бірі осы хеш функцияларға негізделген SPHINCS+ алгоритмі болып табылады. Бұл алгоритмде белгілі бір деректер блогының жиынтыққа жататындығына Мерклдің хеш ағаштарын пайдалану арқылы қол жеткізеді. Дегенмен, Меркл ағашының бірқатар кемшіліктері бар, олардың ең негізгісі аутентификация жолының ұзын болуы. Осы олқылықтарды жою мақсатында, алғаш болып Джон Кушмауло өз еңбегінде Verkle ағашын қолдануды ұсынды [7-8].

Verkle ағашын Меркл ағашының жетілдірілген түрі деп атасақ болады, бірақ бұл жерде, түйіндердегі мәндерді міндеттеу мақсатында векторлық немесе полиномдық міндеттемелер қолданылады. Бұл ұсыныс дәстүрлі Меркл ағашын қолданғаннан қарағанда бірнеше артықшылығы бар. Атап айтсақ, Verkle ағашындағы дәлелдер Меркл ағашымен салыстырғанда айтарлықтай қысқа, верификация процесі аз есептеу ресурстарын талап етеді, қолдану мүмкіндігі де кең. Verkle ағаштары блокчейн жүйелерінде, мәліметтер құрылымдарында және цифрлық қолтаңба жүйелерінде тиімді қолданылануға болады [9].

Векторлық міндеттемелер (vektor commitments) - вектордың мәндерін басқа тараптарға ашпайақ, оның белгілі бір қасиеттерін дәлелдеуге мүмкіндік береді. Бұл әдіс көптеген қолданбаларда, соның ішінде нөлдік дәлелдеулерде, блокчейндерде және тиімді верификация механизмдерінде қолданылады. Дәстүрлі полиномдық міндеттемелер көбінесе Лагранж интерполяциясы немесе коэффициенттік ұсыну арқылы беріледі. Бірақ, мұндай тәсілдерде міндеттеменің өлшемі мен есептеу күрделілігі айтарлықтай жоғары болуы мүмкін. Сонымен қатар, қазіргі көптеген полиномдық міндеттемелер CDH (Computational Diffie-Hellman) немесе RSA сияқты кванттық шабуылдарға осал криптографиялық құрылымдарға негізделген [10].

Біздің мақсатымыз, осы мәселені шешу үшін Verkle ағаштары үшін векторлық мінеттемелер ретінде позициялы емес санау жүйесін қолдану. Бұл тәсілдің негізінде Қытайдың қалдықтар теоремасы (CRT - Chinese Remainder Theorem) жатыр. CRT - бұл бүтін сандардың модульдік қалдықтарын біріктіруге мүмкіндік беретін математикалық теорема. CRT бойынша, егер бізде бірнеше өзара жай сандар болса, онда берілген қалдықтар жүйесін қанағаттандыратын бірегей шешім табуға болады. Бұл теорема жүйелерде күрделі есептеулерді жеңілдету үшін қолданылады, әсіресе модульдік арифметиканы пайдалану арқылы. Сондай-ақ, белгілі бір модульдер жиынына қатысты қалдықтарды пайдаланып сандарды бірмәнді түрде көрсетуге мүмкіндік береді. Бұл қасиет векторлық міндеттемелерді оңтайлы түрде құруға мүмкіндік береді, өйткені позициялы емес ұсыну арқылы олардың мәндерін қысқа әрі тиімді дәлелдеуге болады. Сонымен бірге, осы схемаға хеш функцияларды да қатар қолдану перспективалы тәсіл ретінде ұсынылады және осы арқылы жоғары тиімділікке ие бола отырып, қауіпсіздік деңгейін сақтау [11].

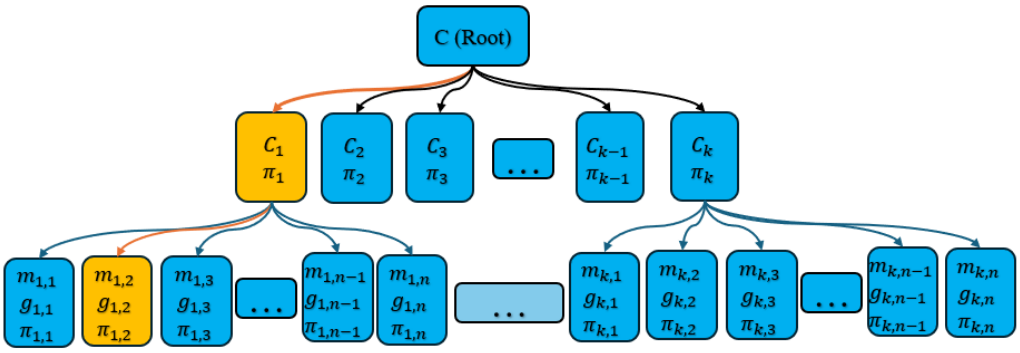
Verkle ағашы тағы бір ерекшелігі – бұл векторлық міндеттемелерді пайдаланумен қатар, дәлелдемелерді полиномдық міндеттемелермен (Polynomial Commitment) де жүзеге асырылу мүмкіндігі бар болуы. Мысалы ретінде KZG міндеттемелерін (Kate-Zaverucha-Goldberg) қарастыруға болады. Полиномдық міндеттемедегі негізгі идея болып барлық еншілес түйіндерді полиномға кодтау және нақты мәндерді жарияламай-ақ еншілес түйіндердің дұрыстығын дәлелдей алу саналады. Әр түйіндегі мәндер бәрі қатысып, полином ретінде ұсынылады, содан кейін оған полиномдық міндеттеме жасалады.

Полиномдық міндеттемелерге негізделген схеманың жұмысы келесідегідей ретпен жүр-

гізіледі: алдымен әрбір түйінді пайдаланып, P(x) полиномы интерполяцияланады. Бұл қадам барлық мәндерге ортақ C міндеттемен жасауға мүмкіндік береді. Одан әрі, кез-келген түйіннің қатысуын дәлелдеу жүргізіледі. Ол үшін жіберуші дәлелдемесін есептейді, бұл мән арқылы келесі қадамда растау үшін тексеру жүргізілетін болады. Дәлелдемені тексеру қадамында тексеруші бисызықтық сәйкестіктерді (pairing operations) қолдана отырып, міндеттеменің дұрыстығын тексереді. Полиномдық міндеттемелер негізінде жұмыс істейтін Verkle ағашы тиімді, ықшам және криптографиялық жағынан сенімді құрылым болып есептеледі. Бұл нұсқа Ethereum 2.0 жүйесінде қолданылу ұсынылуда. Сонымен бірге, ол блокчейн және басқа да криптографиялық жүйелер үшін негізгі стандарттардың біріне айналуда [12].

Бұл жұмыста Verkle ағаштары мен векторлық міндеттемелер негізінде жаңа сандық қолтаңба схемасын әзірлеу ұсынылады. Мұндай тәсілдер хеш-функцияларға негізделген постквантық қауіпсіздік пен тиімділікті үйлестіруге мүмкіндік береді. Постквантық қолтаңбаларды құру үшін векторлық міндеттемелер мен хеш функцияларын біріктіру маңызды рөл атқарады. Векторлық міндеттемелер арқылы қолтаңбалардың дәлдігін тексеруге болады, ал хеш функциялары деректердің тұтастығын қамтамасыз етеді.

Материалдар мен әдістер. Verkle ағаштары блокчейнде кеңінен қолданылатын Меркл-патриция (Merkle Patricia) ағаштарына балама ретінде ұсынылған криптографиялық аутентификация құрылымы.1-суретте ағаш құрылымы кескінделген. Бұл ағаш Меркл (Merkle) ағашына ұқсас, бірақ негізгі айырмашылығы – ол векторлық міндеттемелерді (vector commitments) пайдаланады, бұл оны аз орын алатын әрі жылдам іздеу мүмкіндігін беретін құрылымға айналдырады. Олар тексеруге қажетті деректер көлемін азайтады және желінің тиімділігін арттырады.



1 - сурет. Verkle ағашының құрылымы

Verkle ағашы үш негізгі элементтен тұрады: түйіндер (nodes), әрбір түйін бірнеше ұяшықтан тұратын векторлық міндеттемені қамтиды; векторлық міндеттемелер (vector commitments), түйіндердің мәндерін жинақтап, қысқа криптографиялық міндеттемелер жасауға мүмкіндік береді; жолдар (paths), белгілі бір мәнді дәлелдеу үшін қолданылатын жолдар.

Verkle ағашында әрбір түйіндерден шығатын тармақтардың саны көп болады, бұл тереңдігі аз құрылымды жасауға мүмкіндік береді. Бұл өз кезегінде тексеруге қажетті жолдың қысқаруына алып келеді. Векторлық міндеттемелерді қолдануVerkle ағашының басты ерекшелігі болып табылады. Олар түйін ішіндегі барлық мәндерді жинақтайды және олардың қысқа міндеттемесін жасайды.

Verkle ағашының жұмыс принципі.

Verkle ағашы түйіндердің арасындағы байланысты сақтау үшін міндеттемелерді пайдаланады. Әрбір ұяшықтағы деректер векторлық міндеттеме арқылы бекітіледі. Бұл әдіс, деректерді

аз орын алатын етіп сақтауға, іздеуді жылдамдатуға және желінің жүктемесін азайтуға көмектеседі.

Дәстүрлі Меркл ағаштарында түбірлік хэшті есептеу үшін барлық деңгейдегі хэштерді жинақтау керек. Ал Verkle ағаштарында түбірлік міндеттеме (root commitment) арқылы тек бір ғана жолды дәлелдеуге болады, бұл дәлелдердің көлемін айтарлықтай азайтады.

Verkle ағаштарын қолданудың бірнеше негізгі артықшылықтары бар.

1. Аз орын алу, яғни дәлелдер көлемі кіші болғандықтан, блокчейн желілерінде сақтау тиімділігі жоғары.

2. Дәлелдеу және тексеру процестері жылдамырақ орындалады.

3. Векторлық міндеттемелер сенімді криптографиялық алгоритмдермен қорғалған.

Бірақ, Verkle ағаштарын қолдануда кейбір қиындықтар туындауы мүмкін. Атап айтқанда, векторлық міндеттемелерді есептеу көп ресурстарды қажет етуі мүмкін, сонымен бірге, қазіргі блокчейн жүйелері Меркл ағаштарын қолданады, сондықтан Verkle ағаштарына көшу үшін жаңа архитектура қажет. Блокчейн желілерінде Verkle ағаштарын енгізу үшін хаттамаларды өзгерту қажеттілігі де туындауы мүмкін [13].

Қытайдың қалдықтар теоремасы (ҚҚТ) - модульдік арифметикаға негізделген және сандарды бір-біріне қарапайым модульдер бойынша қалдықтар жиыны ретінде көрсетуге мүмкіндік беретін маңызды математикалық құрал. Бұл теорема криптографияда, кодтау теориясында, есептеуіш математиканың түрлі салаларында және арнайы есептеуіш архитектураларда қолданылады [14].

Позициялы емес санау жүйелері (ПЕСЖ) - бұл сандық мәндерді көрсету үшін санның әрбір разрядындағы мәннің орналасуына тәуелсіз есептеу тәсілі. ПЕСЖ-нің ерекшелігі – әрбір цифр белгілі бір ереже бойынша жеке өңделеді, бұл жүйелерді параллель есептеулерде және үлкен сандармен жұмыс істеуде тиімді етеді. ҚҚТ негізінде құрылған позициялы емес санау жүйесі үлкен сандарды өңдеуде жоғары тиімділікке ие болады [15].

Қытайдың қалдықтар теоремасы модульдік теңдеулер жүйелерін шешу үшін қолданылады және ол келесі түрде беріледі:

Егер $m_1,\ m_2, \dots, m_n$ өзара жай сандар болса, онда кез келген бүтін $a_1,\ a_2, \dots, a_n$ сандары үшін келесі теңдеулер жүйесін шешетін бірегей x бар және ол $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$ модулі бойынша анықталады.

$$\begin{cases} x \equiv a_1 mod m_1 \\ x \equiv a_2 mod m_2 \\ \vdots \\ x \equiv a_n mod m_n \end{cases}$$

Бұл теорема сандарды әртүрлі модульдер бойынша бөлек өңдеуге мүмкіндік береді, бұл үлкен сандармен жұмыс істеуді жеңілдетеді. Криптографияда, сигнал өңдеуде және деректерді кодтауда кеңінен қолданылады.

Аталған теңдеулер жүйесін шешу 4 қадамнан тұрады:

1. Жалпы модульді есептеу:

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_n$$

2. Әрбір модуль үшін қосалқы модульдерді анықтау:

$$M_i = \frac{M}{m_i}$$

3. Кері элементтерді табу:

$$y_i = M_i^{-1} mod m_i$$

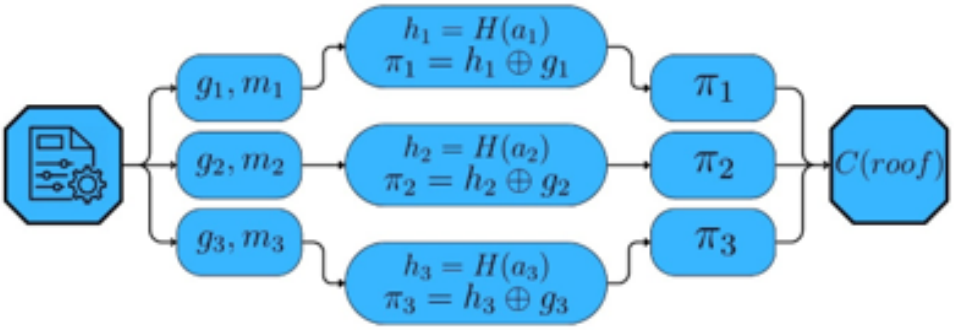
4. Шешімді анықтау:

$$x = \sum_{i=1}^{n} a_i M_i y_i$$

Қытайдың қалдықтар теоремасы мен позициялы емес санау жүйелері математиканың маңызды бағыттары болып табылады. ҚҚТ модульдік арифметиканы тиімді пайдалану арқылы күрделі есептеулерді оңайлатуға көмектеседі. Ал ҚҚЖ позициялы емес санау жүйесінің бір түрі

ретінде үлкен сандармен жұмыс істеуде, параллель есептеулерде және криптографияда ерекше рөл атқарады. Бұл екі тұжырымдаманың байланысы ақпараттық қауіпсіздік пен жоғары өнімділікті есептеулерде үлкен маңызға ие [16-17].

Нәтижелер және талқылау. Verkle ағашы - бұл блокчейн және криптография әлеміндегі жаңашыл деректер құрылымы. Ол дәстүрлі Меркль ағашының кемшіліктерін жою үшін жасалған және деректерді тиімді растау мен сақтауға мүмкіндік береді. Verkle ағашы векторлік міндеттемелер деген математикалық тәсілдерді қолданады, бұл оны әлдеқайда жылдам және ықшам етеді. Біздің зерттеу жұмысымыздың да мақсаты қытайдың қалдықтар теоремасына сүйене отырып векторлық міндеттемелер мен дәлелдемелерді құру.2-суретте Verkle ағашы үшін бір түйін және үш жапырақ жағдайында ПЕСЖ қолданып векторлық міндеттеме құру кескінделген.



2 - сурет. ПЕСЖ негізінде векторлық міндеттеме

Бұл әдіс деректерді тиімді және ықшам түрде ұсынуға мүмкіндік береді. Мұндай жүйелерді құрудың негізгі идеясы – деректерді бірнеше модуль бойынша бөліп, олардың қалдықтарын пайдалану арқылы векторлық міндеттемелерді құру және ол бірнеше қадамнан тұрады.

1. Модульдерді таңдау. Қолданылатын модульдер ретінде жай сандар таңдалады. Жапы жағдайда, ҚҚТ шартына сүйеніп, өзара жай сандар арқылы да құруға болар еді. Бірақ, ағаштың бос жапырақтарын басқа мәндермен толықтыру кезінде жаңа таңдалатын модульдің осыған дейін бар модульдердің бәрімен өзара жай екендігіне салыстыру қажет болады. Сондықтан, модуль ретінде жай сандар таңдап алынды. Яғни, $m_1, m_2, \dots, m_k$ модульдері жай сандар.

2. Псевдокездейсоқ сандар генераторының көмегімен $g_1, g_2, \dots, g_k$ тізбегін аламыз.

3. Verkle ағашының барлық жапырақтарына ортақ C міндеттемені есептеу үшін алдымен барлық жапыраққа тиеселі a_i ақпараттары $H : \{0,1\} \to \{0,1\}^n$ функциясы арқылы хештеледі, $h_i = H(a_i)$. Сонымен бірге, дәлелдеме үшін қажетті ашық π_i параметрі келесідей анықталады: $\pi_i = h_i \oplus g_i$, где $i = \overline{1,k}$.

4. ҚҚТ сүйене отырып ағаштың түбіріне тиеселі, яғни жалпыға ортақ C есептеледі. Бұл жерде, π_i – m_i-лер бойынша қалдық ретінде қарастырылады.

$$C \equiv \pi_i \,(mod m_i)\,, i = \overline{1,k}$$

Бұл теңдеулер жүйесінің шешімі бірегей болады және ол $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$ модулі бойынша анықталады. Шешім келесі формула бойынша табылады:

$$C = \sum_{i=1}^{n} \pi_i M_i M_i^{-1} (mod M)$$

мұндағы, $M_i = \frac{M}{m_i}$, ал M_i^{-1} – модуль m_i бойынша M_i-ге мультипликативті кері элемент.

Сонымен, C – жалпыға ортақ міндеттеме

ретінде, ал π_i-лер ашық параметр ретінде жарияланады.

Верификация алгоритмі π_i-лердің басқа мәндерін ашпай-ақ a_i хабарламасының осы C-ның құрамына кіретінін тексере алады, яғни верификацияның мағынасы белгілі бір түйіннің (node) немесе мәннің Verkle ағашында бар екенін дәлелдеу болып табылады. Сондай-ақ, хабарламаның бүтіндігін немесе өзгермегендігі де тексеріледі. Ол үш қадамнан тұрады:

1. a_i хабарламасына сәйкес (p_i, g_i) дәлелдемесі жіберіледі.

2. $\pi_i = Cmodp_i$ тексеріледі. Егер бұл есептеу дұрыс шықса π_i-дің Verkle ағашында бар екеніне дәлел болады.

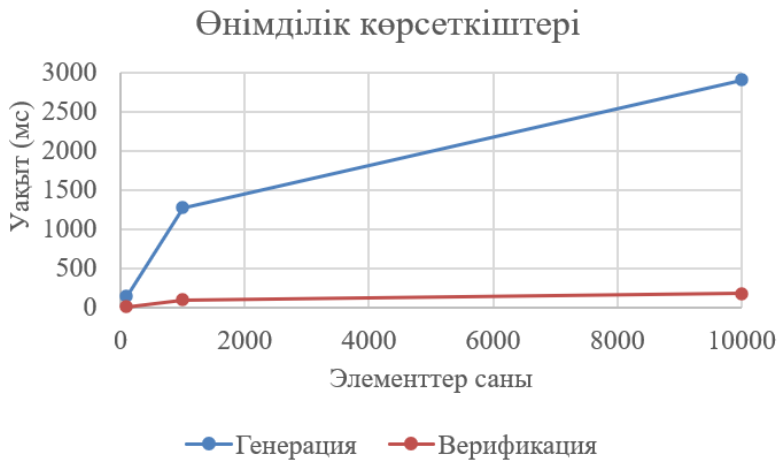
3. $v_i = H(a_i) \oplus g_i$ есептеледі. Егер $\pi_i = v_i$ болса, онда міндеттеме дұрыс және сәйкесінше a_i хабарламасы да өзгеріске түспеген деген тұжырым жасалады.

Осындай жолмен құрылған векторлық міндеттемелердің бір артықшылығы, j-ші хабарламаны жаңартқымыз келсе, яғни басқа хабарламамен ауыстырғымыз келген жағдайда модуль M -ді қайта есептей-ақ C міндеттемесін $C' = \sum_{i=1}^{k} \pi_i' \cdot M_i' \cdot M_i'^{-1} mod M$ қайта есептеуге болады.

Төменде 1-кестеде үш сценарий үшін, яғни бір түйіндегі элементтер (жапырақтар) саны 100, 1000 және 10 000 болғанда Verkle ағашы негізіндегі схеманың жұмыс істеу өнімділігі көрсетілген. Өлшеулер қолтаңба генерация уақыты мен верификация уақыты, сонымен қатар жады тұтыну көрсеткіштері бойынша жасалды.

1 - кесте. Өнімділік көрсеткіштері

Элемент саны	Генерация уақыты (мс)	Верификация уақыты (мс)	Жады тұтынуы (МБ)	көлемі (КБ)
100	146	16	0.05	3.2
1000	1280	102	0.5	32
10000	2912	180	5.1	320



3-сурет. Генерация және верификация бойынша өнімділік көрсетеіштері

Жоғарыда айтқандай, хабарламаның өзгермегендігін тексеру үшін (p_i, g_i) дәлелдемесі жіберіледі және π_iмен v_i есептеледі.1-кестеде келтірілген үш жағдай үшін де бұл параметрлер-

дің көлемі өзгермейді. C міндеттемесінің көлемі ғана өзгереді және өзгерісі эдементтер санына пропорционал болады.3-суретте генерацияға және верификацияға жұмсалатын уақыттардың элемент санына қарай өзгеру динамикасы көрсетілген.

Өнімділікті объективті бағалау үшін бағдарламалық іске асыру Microsoft Visual Studio интеграцияланған әзірлеу ортасында C++ бағдарламалау тілінде жүзеге асырылды. Зерттеу жүргізілген дербес компьютердің сипаттамалары: операциялық жүйе – Windows 10 Pro (22H2 нұсқасы), жүйе түрі – 64-разрядты операциялық жүйе, процессор - Intel(R) Core (TM) i5-7500T CPU @ 2.70GHz 2.70 GHz, жедел жады - 8,00 ГБ.

Векторлық міндеттемелерді қолдану арқылы Verkle ағаштары деректерді жылдам тексеруді қамтамасыз етеді. Бұл әсіресе деректердің аутентификация жылдамдығы маңызды рөл атқаратын таратылған жүйелер үшін өте маңызды. Кванттық шабуылға төзімділік-Verkle ағаштарын болашақ криптографиялық жүйелер үшін перспективалық шешім ететін тағы бір маңызды аспект. Дискретті логарифмнің немесе факторизацияның күрделілігіне негізделген дәстүрлі схемалардан айырмашылығы, олар постквантты криптографиялық механизмдерге бейімделуі мүмкін, бұл олардың ұзақ мерзімді сенімділігін арттырады. Verkle ағаштарының осы қасиеттері жоғары тиімділікті, ықшамдылықты және қауіпсіздікті қажет ететін әртүрлі криптографиялық қолданбалар үшін таңдаулы шешім болады және криптография мен блокчейн технологиясының ең перспективалы бағыттарының біріне айналдырады деп болжанады.

Келесі 2-кестеде ҚҚТ негізінде құрылған Verkle ағашындағы векторлық міндеттемелердің қолдану аймағына қатысты ерекшеліктері көрсетілген. Бұл мәліметтермен қоса осы қолдану аймақтарындағы ҚҚТ-ның өзіндіе қасиеттеріде көрсетілген.

2 - кесте. ҚҚТ-нің Verkle ағашындағы векторлық міндеттемелерде қолданылу ерекшеліктері

Қолдану аймағы	**ҚҚТ ықпалы**	**Verkle ағашындағы ҚҚТ негізіндегі векторлық міндеттемелерге әсері**
Міндеттемелерді есептеуді оңтайландыру кезінде	Үлкен өріс элементтерін бірнеше кіші өрісте есептеуге мүмкіндік береді.	KZG міндеттемелерінің тиімділігін арттырады. Вектордағы әрбір элементті бөлек есептеуге мүмкіндік береді.
Дәлелдеуді жылдамдату кезінде	Қалдықтар жүйесі арқылы есептеулерді параллель жүргізуге болады.	Көпмүшелік дәлелдеулер аз ресурспен орындалады. Вектордағы барлық элементтерді бір уақытта дәлелдеуге мүмкіндік береді.
Деректерді қысу кезінде	Бірнеше шағын мәндерге жіктеп, сақтау тиімділігін арттырады.	Verkle түйіндерінің өлшемін азайтады. Бірнеше элементті бір міндеттемені біріктіру арқылы сақтау кеңістігін үнемдейді.
Қалпына келтіру механизмдерімен жұмыс істегенде	Жоғалған немесе бүлінген деректерді модульдік ақпарат арқылы қалпына келтіру.	Verkle ағашындағы түйіндердің сенімділігін арттырады. Міндеттememен жеке элементтерді қалпына келтіруге мүмкіндік береді.
Zero-Knowledge дәлелдері	Қалдықтар жүйесін қолдану арқылы есептеуді оңайлатады.	zk-SNARKs ішіндегі көпмүшелік дәлелдеуді жақсартады. Векторлық дәлелдерді оңтайландырады

Verkle ағашының есептеу тиімділігін басқа ағаш құрылымдарымен салыстыру төмендегі 3-кестеде көрсетілген.

3 - кесте. Басқа құрылымдармен салыстыру кестесі

Ағаш түрі	Дәлел ұзындығы	Ықшамдылық
Merkle ағашы	$O(\log_2 n)$	Төмен
Patricia ағашы	$O(\log_2 n)$	Орташа
Verkle ағашы	$O(1)$	Жоғары

Деректерді қысу бастапқы ақпаратты жоғалтпай, оны ықшамдау процесі. Бұл әдіс сақтау кеңістігін азайтуға және деректерді жылдамырақ тасымалдауға мүмкіндік береді. Verkle ағашындағы деректерді қысу – міндеттемелерді сақтау кезінде орын алатын құрылымдық оңтайландыруды білдіреді. Бұл процесс бірнеше негізгі тәсілдер арқылы жүзеге асады:

- Verkle ағаштары деректерді вектор түрінде көрсетіп, міндеттемелердің қысқа болуын қамтамасыз етеді. Бұл Merkle ағашына қарағанда аз кеңістік қажет етеді.

- Қытайдың қалдықтар теоремасы негізінде модульдік арифметика қолдану арқылы деректердің өлшемін кішірейтуге болады.

- *O(1)* күрделілікпен дәлел ұсыну, яғни дәлелдер ұзындығы тұрақты болғандықтан, оларды сақтау және тексеру үшін аз орын қажет.

Verkle ағашы Merkle және Patricia ағаштарымен салыстырғанда қысқа міндеттемелер арқылы есептеу тиімділігін арттырады, бұл желілерде жүктемені азайтуға және блокчейн жүйесінде транзакция жылдамдығын арттыруға мүмкіндік береді.

Қауіпсіздік аспектілері. Құрылған міндеттеменің беріктілігін бағалау үшін байланыстылық (binding), жасырындылық (hiding) және шабуылдарға беріктілік тұрғысынан қарастырайық.

1. Байланыстылық (Binding Property), басқаша айтқанда міндеттеме ашылғаннан кейін оны өзгерту мүмкін бе?

Егер шабуылшы C мәнін өзгертпей-ақ басқа π_i-лерге сәйкес келетін жаңа бастапқы дерек таба алса, міндеттеменің байланыстылығы бұзылады.

ҚҚТ ерекшелігі теңдеулер жүйесінде қолданылатын модульдер өзара жай сандар болса шешімі бірегей болады. Яғни, бірдей модульдер жиыны үшін C мәні өзгермейді. Біздің жағдайда, $m_1, m_2, \dots, m_k$ модульдері жай сандар болғандықтан, $C \equiv \pi_i \, (mod m_i)$ теңдеулер жүйесінің бір ғана шешімі бар және бұл міндеттемені қайта есептегенде сол мәннің өзін алатынымызды білдіреді.

Егер модульдер өзара жай болмаса, онда теңдеулер жүйесінің бірнеше шешімі болуы мүмкін еді, бұл міндеттемені өзгертуге мүмкіндік береді. Сонымен бірге, модульдер тым кіші болса, міндеттемені бұзу оңайырақ болады.

Қорыта айтқанда, егер $m_1, m_2, \dots, m_k$ үлкен және жай сандар болса, байланыстылық (binding) сақталады.

2. Жасырындылық (Hiding Property), яғни міндеттемені көріп, бастапқы деректі білуге мүмкіндігін қарастыру.

ҚҚТ негізіндегі міндеттемеде жасырындылық келесідей қамтамасыз етіледі:

- Ашық параметр $\pi_i = h_i \oplus g_i$ түрінде берілген.

- g_i псевдокездейсоқ болғандықтан, π_i мәнінен бастапқы деректі алу қиын.

Қандай жағдайда осалдық танытуы мүмкін:

1. Егер g_i-ді алуда әлсіз генератор қолданылса немесе болжамды болса, шабуылшы h_i-ды табу мүмкіндігі бар.

2. Егер модульдер өте кіші болса, шабуылшы міндеттемені брутфорс арқылы тексере алады.

Жасырындылыққа берік болу үшін:

- g_i мықты криптографиялық псевдокездейсоқ генератор арқылы жасалуы қажет.

- Модульдер жеткілікті үлкен болуы қажет.

3. Шабуылдарға тұрақтылық (Attack Resistance).

а) Кері есептеу шабуылы (Reverse Engineering Attack)

Міндеттемені біле отырып, бастапқы деректі қалпына келтіру мүмкін бе?

ҚҚТ теңдеуі:

$$C \equiv \pi_i \left(mod m_i\right), i = \overline{1,k}$$

Егер k-нің мәні кіші болса, C-ны көріп, барлық мүмкін π_i-лерді тексеруге болады.

Бұдан қорғану үшін: Үлкен k таңдау (мысалы, $k \geq 5$); Үлкен m_i таңдау (мысалы, 256-биттік жай сандар).

ә) Міндеттемені қолдан жасау шабуылы (Forgery Attack)

Басқа біреудің міндеттемесіне сәйкес келетін жаңа мән жасау мүмкін бе?

ҚҚТ жүйесі бірегей шешім береді, сондықтан міндеттемені қолдан жасау үшін:

- Жалған π'_i таңдау керек, бірақ олардан C қайта есептелгенде бұрынғыдай шығуы қажет.

- Бұл $m_1, m_2, \ldots, m_k$ өзара жай болғанда мүмкін емес.

б) Модульдер таңдау осалдығы (Small Moduli Attack)

Егер модульдер өте кіші болса не болады?

Егер модульдер өте кіші болса, шабуылшы міндеттеменің мүмкін мәндерін брутфорс арқылы тексеріп, h_i-ді табу мүмкіндігі бар. Бірақ, h_i бастапқы ақпараттың хеш мәні болғандықтан ақпараттың өзіне қол жеткізе алмайды.

Осы талдаулардың нәтижесінде, құрылған алгоритмнің шабуылдарға берік болуы үшін кем дегенде әр m_i үшін 256-биттік жай сандарды және k-ны 5-тен жоғары етіп таңдау қажет.

4-кестеде модуль ұзындығының (бит бойынша) есептеу уақыты, жад тұтынуы және қауіпсіздік деңгейіне әсері көрсетілген. Мәліметтер $k = 100$ болған жағдайда есептелінді.

4 - кесте. Әртүрлі модуль ұзындықтарының салыстырмасы

Модуль ұзындығы (бит)	Есептеу уақыты (мс)	Жады тұтынуы (МБ)	Қауіпсіздік деңгейі
128	15	0.03	Орташа
256	146	0.05	Жоғары
512	2364	0.1	Өте жоғары

Жалпы алғанда, модуль неғұрлым үлкен болса, байланыстылық және жасырындылық қасиеттері күшейеді, яғни, міндеттемені бұзу немесе бастапқы деректі табу қиындайды. Бірақ үлкен модульдер: есептеу уақытын ұзартады (операциялар ауырлайды); көбірек жад тұтынады; кей жағдайда тым үлкен модуль (1024 бит және одан жоғары) практикалық тұрғыда тиімсіз болады. Сондықтан 256 бит (немесе 512 бит) қазіргі NIST (National Institute of Standards and Technology) стандарттарына сай ең оңтайлы таңдау болып есептеледі.

Қорытынды. Verkle ағаштары – бұл заманауи криптографиялық деректер құрылымдарының маңызды элементі, әсіресе блокчейн технологиясында масштабтау мәселелерін шешуге бағытталған. Олардың негізгі артықшылығы векторлық міндеттемелер арқылы үлкен деректер жиынтығын қысқаша және тиімді түрде растауға мүмкіндік беруі. Бұл мақалада біз Verkle ағаштарындағы векторлық міндеттемел құрудың артықшылықтарын, соның ішінде Қытайдың қалдықтар теоремасына және позициялы емес санау жүйелері сияқты математикалық тұжырымдарды қолданудың тиімділігін қарастырдық.

Бұл зерттеуде ұсынылған схеманы жүзеге асыру үшін нақты криптографиялық алгоритмдер мен параметрлер таңдалды. Атап айтқанда, схемада SHA3-256 криптографиялық хеш-функциясы қолданылды, яғни оның жұмыс нәтижесі 256 биттік хеш мәнін береді. Ол қазіргі уақытта кеңінен зерттелген, постквантық қауіпсіздікке сай және деректердің тұтастығы мен аутентификациясын сенімді қамтамасыз етеді. Міндеттемелерді есептеу үшін пайдаланылған модульдер ұзындығыда осы хеш мәндерге сәйкес 256 бит болып таңдалды. Бұл көрсеткіш есептеу тиімділігі мен қауіпсіздік деңгейінің оңтайлы теңгерімін береді.

Verkle ағаштарының негізгі ерекшеліктері: Орталықтандырылмаған деректерді жинақтау, яғни әрбір түйін векторлық міндеттемелердің көмегімен деректерді қысылған түрде сақтайды; Түбірлік мәнді пайдалану арқылы дәлелдеу уақыты қысқарады; Масштабталу мүмкіндігі бар, үлкен деректер жиынтығын сақтау және тексеру оңай болады. Verkle ағаштары көбінесе блокчейн технологиясында қолданылады, себебі олар қысқа дәлелдер арқылы желідегі түйіндердің жүктемесін азайтуға көмектеседі.

Қытайдың қалдықтар теоремасы модульдік арифметикаға негізделген және үлкен сандарды бірнеше кіші модульдер жиынтығы ретінде көрсетуге мүмкіндік береді. Бұл қасиет Verkle ағаштарындағы міндеттемелерді оңтайландыруға ықпал етеді.

Позициялы емес санау жүйелері сандарды көрсету әдісі ретінде Verkle ағаштарының тиімділігін арттыруға көмектеседі. Әсіресе, қалдықтар кластарының жүйесі Verkle міндеттемелеріне қолайлы. Verkle ағаштарында үлкен көлемдегі деректерді қысу маңызды. ҚҚЖ арқылы әрбір түйіндегі деректер модульдік мәндер ретінде сақталып, жалпы деректер құрылымының сыйымдылығы оңтайландырылады. Векторлық міндеттемелер құруда ПЕСЖ-нің қасиеттерін пайдалану міндеттемелерді тез генерациялауға мүмкіндік береді.

Бұл тәсілдердің нәтижесінде Verkle міндеттемелері жоғары тиімділікті, қауіпсіздікті және деректерді өңдеудің жылдамдығын қамтамасыз ететін қуатты құралға айналады. Verkle ағаштарының болашағы олардың блокчейн технологиясында кеңінен қолданылу мүмкіндігіне байланысты. Қысқа дәлелдер мен тиімді міндеттемелердің арқасында олар үлкен масштабтағы желілерде түйіндердің жүктемесін азайтуға көмектеседі. Блокчейн экожүйесінде Verkle ағаштарын енгізу желінің жылдамдығын арттырумен қатар, есептеу ресурстарын үнемдеуге және транзакциялардың тиімділігін жақсартуға мүмкіндік береді. Сондай-ақ, олар блокчейндердің орталықтандырылмаған табиғатын сақтай отырып, масштабталу мәселелерін шешудің жаңа тәсілдерін ұсынады. Құпиялылық пен деректерді қорғау саласында Verkle ағаштары маңызды рөл атқара алады, себебі олар міндеттемелердің қауіпсіздігін арттырып, деректерді тиімді басқаруға жағдай жасайды. Осы артықшылықтардың арқасында Verkle ағаштары болашақта блокчейн жүйелерінің ажырамас бөлігіне айналып, жаңа шешімдердің негізі бола алады.

Постквантық алгоритмдердің негізгі бағыттарының бірі торларға негізделген криптография болып табылады. Осыған байланысты алдағы зерттеулерде векторлық міндеттемелерді дәл осы теория негізінде құру және мақалада ұсынылған әдіспен жан-жақты салыстыру жоспарлануда. Салыстыру барысында міндеттеменің өлшемі, дәлел ұзындығы, дәлелдеу мен тексеру уақыты, есептеу күрделілігі, жады талаптары және қауіпсіздік деңгейі сияқты негізгі параметрлер ескеріледі. Бұл салыстыру қай тәсілдің тиімділігін жан-жақты анықтауға мүмкіндік береді. Ең нәтижелі деп танылған шешім одан әрі жетілдіріліп, аппараттық деңгейде жүзеге асыруға бейімделеді және аппараттық оңтайландыру жолдары қарастырылатын болады.

Қаржыландыру. *Бұл мақала AP23488112 «Verkle ағашы негізінде кванттық төзімді цифрлық қолтаңба схемасын құру және зерттеу» гранттық қаржыландыру жобасы негізінде жүргізілді.*

Әдебиеттер

1. Cotan P. and Teşeleanu G. A security analysis of two classes of RSA-like cryptosystems // Journal of Mathematical Cryptology. - 2024. - Vol.18 (1): 20240013. DOI 10.1515/jmc-2024-0013.

2. Wardhani R. W., Septono Catur Putranto D., Cho J. and Kim H. A Highly Efficient ECPM Quantum Circuit for Binary Elliptic Curve Cryptanalysis // IEEE Access. - 2024. - Vol.12. - P.161569-161583. DOI 10.1109/ACCESS.2024.3489552.

3. Larasati H. T. and Kim H. Quantum cryptanalysis landscape of shor'salgorithm for elliptic curve discrete logarithm problem // International Conference on Information Security Applications. – 2021. - Springer. - P.91-104. DOI 10.1007/978-3-030-89432-0_8.

4. Putranto D.S.C., Wardhani R.W., Larasati H.T., Ji J. and Kim H. Depth-optimization of quantum cryptanalysis on binary elliptic curves // IEEE Access. - 2023.- Vol.11. -P.45083–45097. DOI 10.1109/ACCESS.2023.3273601.

5. Algazy K., Sakan K., Khompysh A., Dyusenbayev D. Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1 // Computers.- 2024. -Vol.13(1):26.- P.1-14. DOI 10.3390/computers13010026.

6. Algazy K., Sakan K., Nyssanbayeva S. and Lizunov O. Syrga2: Post-Quantum Hash-Based Signature Scheme//Computation.-2024.-Vol.12(125).- P.1-17. DOI 10.3390/computation12060125.

7. Buchmann J., Dahmen E., Szydlo M. Hash-based Digital Signature Schemes // Post-Quantum Cryptography. - 2009.-P.35-93. DOI 10.1007/978-3-540-88702-7_3.

8. Lee J., Park Y. HORSIC+: An Efficient Post-Quantum Few-Time Signature Scheme // Applied Science. - 2021. - Vol.11 (16): 7350. DOI 10.3390/app11167350.

9. Kuszmaul J. Verkle trees. - 2019. - P.1–12. https://math.mit.edu Kuszmaul.pdf.- Қаралған күні: 22.04.2024.

10. Kuznetsov O., Kanonik D., Rusnak A., Yezhov A., Domin O., Kuznetsova K. Adaptive Merkle trees for enhanced blockchain scalability // Internet of Things. - 2024. - Vol.27: 101315. DOI 10.1016/j.iot.2024.101315.

11. Bünz B., Bootle J., Boneh D., Poelstra A., Wuille P. and Maxwell G. Bulletproofs: Short Proofs for Confidential Transactions and More // IEEE Symposium on Security and Privacy (SP). - San Francisco. - 2018. - P.315-334. DOI 10.1109/SP.2018.00020.

12. Zhao X., Zhang G., Long H.-W., Si Y.-W. Minimizing block incentive volatility through Verkle tree-based dynamic transaction storage // Decision Support Systems. – 2024. – Vol.180: 114180. DOI 10.1016/j.dss.2024.114180.

13. Iavich M., Kuchukhidze T., Bocu R. A Post-Quantum Digital Signature Using Verkle Trees and Lattices // Symmetry. - 2023. - Vol.15 (12): 2165. DOI 10.3390/sym15122165.

14. Chang C. -H., Molahosseini A. S., Zarandi A. A. E. and Tay T. F. Residue Number Systems: A New Paradigm to Datapath Optimization for Low-Power and High-Performance Digital Signal Processing Applications // IEEE Circuits and Systems Magazine. – 2015. – Vol.15 (4). - P.26-44. DOI 10.1109/MCAS.2015.2484118.

15. Omondi A. and Premkumar B. Residue Number Systems: Theory and Implementation // Advances in Computer Science and Engineering: Texts – 2007. –Vol.2. DOI 10.1142/p523.

16. Biyashev R.G., Kalimoldayev M.N., Nyssanbayeva S.E., Kapalova N.A., Dyusenbayev D.S., Algazy K.T. Development and analysis of the encryption algorithm in nonpositional polynomial notations // Eurasian Journal of Mathematical and Computer Applications. - 2018. -T.6(2). – P.19-33. DOI 10.32523/2306-6172-2018-6-2-19-33.

17. Biyashev R.G, Kapalova N.A, Duysenbayev D.S, Algazy K.T, Wojcik W., Smolarz A. Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network // International journal of electronics and telecommunications. – 2021. Vol.67 (1). - P.127-132. DOI 10.24425/ijet.2021.135954.

Авторлар туралы мәліметтер

Алғазы К.Т. - PhD, қауымдастырылған профессор, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, e-mail: kunbolat@mail.ru;

Сақан Қ.С. - PhD, аға ғылыми қызметкер, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, e-mail: kairat_sks@mail.ru;

Капалова Н.А. - техника ғылымдарының кандидаты, қауымдастырылған профессор, Ақпараттық және есептеу технологиялары институты, Алматы, Қазақстан, e-mail: nkapalova@mail.ru;

Алимжан Е.Ж. әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: ayerkebulan19@gmail.com.

Information about the authors

K. Algazy - PhD, associate professor, Institute of information and computational technologies, Almaty, Kazakhstan, e-mail: kunbolat@mail.ru;

K. Sakan - PhD, senior researcher, Institute of information and computational technologies, Almaty, Kazakhstan, e-mail: kairat_sks@mail.ru;

N. Kapalova - candidate of technical sciences, associate professor, Institute of information and computational technologies, Almaty, Kazakhstan, e-mail: nkapalova@mail.ru;.

Y. Alimzhan - master’s student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: ayerkebulan19@gmail.com.