Сведения об авторах

Мамырбек Аукебайулы Бейсенби – профессор, доктор технических наук кафедры «Системного анализа и управления», Евразийский национальный университет им. Л.Н. Гумилева, Республика Казахстан; e-mail: beisenbi_ma@enu.kz. ORCID: https://orcid.org/0000-0003-2109-4512.

Акерке Адилхановна Ауелбаева* – докторант PhD по образовательной программе «Автоматизация и управление» кафедры «Системного анализа и управления», Евразийский национальный университет им. Л.Н. Гумилева; преподаватель Высшей школы интеллектуальных систем, Astana IT University, Республика Казахстан. ORCID: https://orcid.org/0009-0000-0433-1075.

Владимир Владимирович Никулин – PhD, профессор Государственного университета штата Нью-Йорк в Бингемтоне (State University of New York at Binghamton), Соединенные Штаты Америки, Binghamton, NY 13902. ORCID: https://orcid.org/0000-0002-6504-8270.

Салтанат Шамшиевна Бейсембина – регистратор и генеральный директор по академическим делам, Назарбаев Университет, Астана, Республика Казахстан; e-mail: Saltanat.Shamshiyeva@nu.edu.kz. ORCID: https://orcid.org/0000-0003-4482-8531.

Received 30.03.2026
Revised 29.05.2026
Accepted 02.06.2026

https://doi.org/10.53360/2788-7995-2026-3(23)-2

BY 4.0
Check for updates

ҒТАХР: 10.23.01

Н.А. Модовов[1], Н.О. Мекебаев[1,2*], А.Б.Тлеубаева[3], Ө.М.Белғожа[2], І.Садықжан[2]
[1]әл-Фараби атындағы Қазақ ұлттық университеті,
050040, Қазақстан, Алматы қ., әл-Фараби даңғылы, 71
[2]Қазақ ұлттық қыздар педагогикалық университеті,
050000, Қазақстан, Алматы қ., Гоголь көшесі, 114
[3]Шәкәрім университеті,
071412, Қазақстан, Семей қ., Глинка көшесі 20 А
*e-mail: nurbapa80@gmail.com

КРИПТОГРАФИЯЛЫҚ ХАТТАМА: ИНТЕРАКТИВТІ ЕМЕС НӨЛДІК ЖАРИЯ ЕТІЛГЕН ДӘЛЕЛДЕМЕЛЕРДІҢ ЕСЕПТЕУ КҮРДЕЛІЛІГІН ТАЛДАУ

Аңдатпа: *Бұл мақалада интерактивті емес нөлдік жария етілген дәлелдемелердің есептеу күрделілігін ресми тұрғыдан және асимптоталық талдау қарастырылады. Интерактивті емес нөлдік жария етілген дәлелдемелер дәлелдеушіге белгілі бір хабарламаның дұрыстығын, осы хабарламаны тексерушіге қосымша ақпараттарды жасырын дәлелдеуге мүмкіндік береді. Үйлестірілген жүйелерде жиі пайдаланылады. Зерттеуімізде интерактивті емес нөлдік жария етілген дәлелдемелердің сұлбаларының алғашқы базалық мәндер CRS моделында қарастырылады. Есептеу күрделілігін бағалауда негізігі базалық мәндер есебінде дәлелдеу және тексеру куәгердің өлшемі, дәлелдеу көлемі және алгоритмнің уақыт күрделілігі есептелінеді. Көпмүшелік есептеу моделі арқылы алгоритмдердің тиімділігі талданады. Тексеруші алгоритм күрделілігі және дәлелденушінің есептеу күрделілігі дәлдеменеің ұзындығымен анықталады. Дәлелдемелердің асимптоталық көрсеткіштер олардың қолданбалы нәтижелерге әсері зерттеледі. Нәтижелер негізінде интерактивті емес нөлдік жария етілген дәлелдемелердің айырмашылықтары мен ұқсастықтарын талдаудың әдіснамалық негізін және жоғары есептеу өнімділігі бар криптографиялық хаттамаларды жасауды қамтамасыз етеді.*

Талдау нәтижелері көрсеткендей алгоритмдердің есептеу күрделілігі куәгердің көрсеткішіне елеулі түрде тәуелдікті, ал дәлелдеудің ұзындығы тексеру алгоритмінің күрделілігін айқындайды. Бұға қоса, дәлелдеменің асимптоталық көлемдері олардың мәліметтер шығынына тигізетін ықпалы талданды. Осы алынған нәтижелер интерактивті емес нөлдік жария етілген дәлелдемелерді айырмашылықтары мен ұқсастықтарын талдау мен есептеу қолайлы криптографиялық хаттамаларды жасау үшін әдіснамалық негіз ретінде қолданылуы мүмкін.

©Н.А. Модовов, Н.О. Мекебаев, А.Б.Тлеубаева, Ө.М.Белғожа, І.Садықжан, 2026

Түйін сөздер: *Дәлдеуші алгоритм, тексеруші алгоритм, интерактивті емес нөлдік жария етілген дәлелдемелер, криптография, есептеу күрделілігі.*

Кіріспе

Қазіргі цифрлық ортада ақпараттарды сақтау және қорғап тұру, қауіпсіздік деңгейін, құпиялықты мүмкіндігінше қамтамасыз ету криптография саласындағы негізгі зерттеу бағыттарының бірі болып қалыптасты. Бұлттық сервистерде, ашық немесе үлестірілген жүйелерде сенімді өзара байланыс орнату барысында қолданушының жеке базалық мәліметтерін, жеке кілттерін немесе өңдеу көрсеткіштерін ашпай-ақ белгілі бір нәтижені растау қажеттілігі туындайды. Осы тұрғыда нөлдік жария етілген дәлелдер криптография саласындағы аса маңызды әрі болашағы айқын құралының бірі болып есептеледі [1].

Нөлдік жарияланатын дәлелдердің басты мәні – дәлелдеуші тексерушіні белгілі бір тұжырымның шынайылығына иландырады, алайда тексеруші дәлелденген тұжырым жайлы қосымша мәліметке ие болмайды. Бұл әдіс стандартты сәйкестендіру тәсілдері мен тексеру тәсілдерінен түбегейлі өзгеше болып келеді және құпиялылықтың жоғары деңгейін сақтауға мүмкіндік береді [2].

Нөлдік жария етілетін дәлелдер көпшілікке ашық және бастапқы айғақтар екіжақты байланысқа негізделген түрде беріледі. Нөлдік жария етілген дәлелдемелер растаушы тараппен тексеруші тарап арасындағы өзара іс-қимылдың бірнеше кезеңдерін қамтиды. Бұл типтегі хаттамалар ғылыми тұжырым тұрғысынан тиімді көрінгенімен,практикада бірқатар шектеулер байқалады. Нақтырақ айтқанда, өзара әрекеттесуші хаттамалар желідегі кідірістерге байланысты, бір мезгілдегі байланысты қажет етеді және кейбір жағдайларда ауқымдылығы жағынан әлсіз болып келеді [3].

Бұл проблемаларды еңсеру мақсатында интерактивті емес нөлдік жарияланатын дәлелдер ұғымы ұсынылды. Интерактивті емес үлгіде дәлелдеуші дәлелдемені бір рет жасайды және оны тексерушіге жібереді, ал тексеруші оны оны тексеретін тарапқа жолдайды, ал тексеретін тарап оны қосымша сұраусыз-ақ тексере береді. Осы әдіс блокчейн технологияларында, цифрлық дауыс беру жүйелерінде, жасырын сәйкестендіруде және құпия операцияларда кең түрде пайдаланылады [4].

Интерактивті емес нөлдік жария етілмейтін дәлелдердің қолданбалы маңызы олардың есептеу және байланыс тиімділігімен тікелей байланысты. Дегенмен оларды құрастыру мен жүзеге асыру барысында зерттеудің басты нысанына айналатын мәселе – тиімділік болып табылады Өйткені интерактивті емес нөлдік жария етілетін дәлелдер хаттамалары негізінен күрделі математикалық құрылымдарға, криптографиялық хэш алгоритмдеріне, эллиптикалық қисықтарға және көпмүшелік уақыттағы есептеулерге негізделеді. Сол себепті мұндай дәлелдердің есептеу қиындығын талдау олардың қауіпсіздік деңгейін, орындалу жылдамдығын және масштабталуын бағалаудың маңызды құрамдас бөлігі болып саналады [5].

Нөлдік жария етілген дәлелдемелер – бұл дегеніміз бір қатысушыға, яғни дәлелдеушіге, екінші қатысушыға, яғни тексерушіге қандай да бір тұжырымның не себепті ақиқат екенін немесе оны қандай деректер дәлелдейтінін ашпай-ақ оның шын екенін растауға мүмкіндік беретін криптографиялық тәсіл. Нөлдік жария етілген дәлелдемелерді қолдану идеясын 1987 жылы алғаш рет Уриэль Фейг, Амос Фиат және Ади Шамир ұсынған. Бұл жағдайда пайдаланушы өзінің жеке кілтін білетінін көрсетеді, ол құпия күйінде сақталады және жария етілмейді. Осылайша олар өз тұлғасын растауға мүмкіндік алады.

Нөлдік жария етілген дәлелдемелердің басты екі категориясы бар: интерактивті және интерактивті емес.

Нөлдік жария етілген дәлелдемелерге тән негізгі үш қасиет міндетті түрде сақталуы тиіс. Бұл қасиеттер жүйенің сенімділігі мен қауіпсіздігін қамтамасыз етуде шешуші рөл атқарады:

Толықтық**:** Егер пайымдау ақиқат болса, дәлелдеуші тексерушіні оның дұрыстығына толықтай сендіре алады.

Дұрыстық: Егер пайымдау жалған болса, тіпті адал емес дәлелдеуші де тексерушіні тек өте төмен ықтималдық жағдайында ғана иландыра алады.

Нөлдік білім: Егер пайымдау рас болса, тіпті сенімсіз тексеруші де оның шын екендігі туралы қосымша ақпарат ала алмайды.

Интерактивті емес нөлдік жария етілген дәлелдемелер (NIZKP) интерактивті нөлдік жария етілген дәлелдемелерден басты айырмашылығы ретінде дәлел ұсынушы мен тексеру жүргізуші тарап арасында өзара байланыс әрекетінің болмауымен сипатталады. Дәлел ұсынушы дербес дәлелді қалыптастырады, оны тексеру жүргізуші тарап кейіннен қосымша байланыссыз-ақ өз бетінше тексере алады. Бұл процесс көбіне өзара әрекеттесетін нөлдік жария етілетін дәлелдерге қарағанда әлдеқайда ұтымды әрі қолайлы болып келеді, себебі бір мезгілде желіге қосылып тұруды немесе бірнеше рет хабарлама алмасуды талап етпейді. Нөлдік жария етілетін дәлелдерге қол жеткізудің кеңінен қолданылатын тәсілдерінің бірі – цифрлық қолтаңбаларға сүйенетін Fiat–Shamir әдісі болып табылады.

Зерттеу әдістері

Аталмыш зерттеу zk-SNAR·K хаттамаларындағы қазіргі алгоритмдерде жиі пайдаланылатын ортақ алғашқы параметрлерге негізделген үлгідегі интерактивті емес нөлдік жария етілген дәлелдемелерді зерттейді [6]. Сондай-ақ, салыстырмалы зерттеу мақсатында сенімді орнатуды талап етпейтін заманауи zk-SNAR·K хаттамалары қарастырылады [7].

Дәлелдеме көлемі мен бақылаудың күрделілік деңгейін талдау кезінде Bulletproofs жүйесінің дәлелдеме ұзындығының логарифмдік тәуелдігі негізделеді [8]. Басым бөлігі zk-SNARK құрылымдарының методологиялық базасы тұрғысынан арифметикалық схмеалар мен квадраттық магистральды бағдарлама модельдері пайдаланылады [9].

Интерактивті емес нөлдік жария етілген дәлелдемелер қауіпсіздік қасиеттері есептеу жағынан сенімді дәлелдемелер тұжырымдамасына негізделген [10]. Ықшам интерактивті емес дәлелдердің ресми сипаттамасы және олардың қауіпсіздік қасиеттерін негіздеу қазіргі криптографиялық зерттеу жұмыстарында маңызды рөл атқарады [11].

Зерттеу қорытындыларын саралауда ықшам интерактивті емес дәлелдерді верификациялаудың нәтижелілігі олардың тәжірибелік маңыздылығы ретінде қаралды [12]. Қауіпсіздік сипаттамаларын беру үшін интерактивті және интерактивті емес дәлелдеу құрылымдарына ресми қауіпсіздік үлгілері қолданылады [13].

Қарастырылып отырған зерттеуде пайдаланылатын есептеу қиындығына қатысты негізгі анықтамалар мен ұғымдар заманауи криптография оқу құралдарында берілген классикалық түсініктерге сүйенген [14]. Бұған қоса, криптографиялық ережелердің өнімділігін бағалаудың стандартты үлгісі ретінде көпмүшелік есептеу моделі алынды [15].

Интерактивті емес нөлдік жария етілген дәлелдемелер және олардың алгоритмдік қиындығы қарастырылып отырған зерттеудің басты нысаны ретінде есептеледі. Аталған зерттеу шеңберінде интерактивті емес нөлдік жария етілген дәлелдемелер схемасы криптографиялық хаттамалар негізінде зерттеліп, олардың тексеруші және дәлел ұсынушы тараптарындағы есептеу шығындары формальды түрде талданады.

Интерактивті емес нөлдік жария етілген дәлелдемелер схемасы келесі үш алгоритм тұратын жиынтығы ретінде формальді түрде анықталады:

$$NIZK = (\cdot Setup \cdot, \cdot Verify \cdot, \cdot Prove \cdot)$$

мұндағы: $Prove$ – куәгердің негізінде дәлелдеу құратын алгоритм; $Setup$ – жалпы бастапқы параметрлерді генерациялау алгоритмі; $Verify$ – тексеруші дәлелдеменің дұрыстығы мен жарамдылығын тексеруді жүзеге асыратын алгоритм.

Осы зерттеуімізде жоғарыдағы алгоритмдердің тиімділіктің көпмүшелік тиімді есептеу моделі ауқымында қарасытырлады. Яғни, нөлдік қосындысы бар интерактивті емес дәлелдеу және тесеру алгоритмдерінің орындалу уақыты есептің кіріс деректерінің өлшемінен көпмүшелік функциямен шектеледі. Мұндай модель криптографиялық хаттамалардың практикалық іске асырылуын қамтамасыз ететін стандартты есептеу моделі болып табылады. Формальді түрде төмендегідей жазылады:

$$P(m) \in Q(poly(n))$$

Есептеу күрделілігін бағалау әдісі

Бұл зерттеу жұмысында дәлелдеу механизмнің уақыттық $|m|$ тапсырмасының өлшеміне және $|w|$ куәгерінің өлшеміне тәуелді ретінде қарастырылады, ал тексеру механизмінің күрделілігі $|\pi|$ дәлелінің ұзындығымен сипатталады. Интерактивті емес нөлдік жария етілген дәлелдемелер схемамсы үшін $|w|$ және $|\pi|$ ұпайлары есептің өлшеміне қатысты көпмүшеліктермен шектелуі керек.

Классикалық түрде дәлелдеуші алгоритмнің уақыты келесідей есептеледі:

$$P_T = P_T(m, |w|)$$

дәлелденушінің уақыттық күрделілігі есептің өлшеміне m, куәгердің өлшеміне $|w|$ тәелді. Осыны ескере отырып келесідей жазамыз:

$$P_T(m, |w|) \in Q(poly(m, +|w|))$$

мұндағы $|w|$ дәлелдеушіге түсетін негізгі жүктемені сипаттайды.

Дәлелдеме өлшемдері мен куәгерге қойылатын талаптар келсідей. Интерактивті емес нөлдік жария етілген дәлелдемелер, NP – класына жататын есептеулер үшін құрылады.

$$y \in K \leftrightarrow \exists w : R(y, w) = 1$$

мұндағы R – көпмүшелік уақытта тексерілетін қатынас. Осы анықтамаға сәйкес куәгердің өлшемі есептің өлшеміне қатысты көпмүшелікпен шектелуыі тиіс:

$$|w| \leq poly\ (m)$$

Сол сияқты дәлелдеменің ұзындығы да есептің өлшеміне қатысты көпмүшелікпен шектеледі:

$$|\pi| \leq poly\ (m)$$

Келесіде біздер зерттеуде дәлелдеушінің есептеу күрделілігі мен тексерушінің есептеу күрделілігін, дәлелдеме өлшемінің асимптоталық бағалауды қарастыратын боламыз.

Дәлелдеушінің есептеу күрделілігі осы схеманың нақты құрылымына байланыстыда өзгереді. Көпмүшелік міндеттемелер мен арифметикалық схемаларға негізделген интерактивті емес нөлдік жария етілген дәлелдемелер жүйелерінде дәлелдеуші көпмүшелікті интерполяциялайды, хэш функциялары есептеулер мен топтық операцияларды орындайды (Кесте 1). 1 – ші формулада дәлелдеушіге түсетін жүктеменің негізгі шектеуші фактор екенін көрсетеді.

$$P_T(m) = \begin{cases} Q(m^2), & zk - SNARK \\ Q(m\ logm), & zk - SNARK, Bulletpoofs \end{cases}$$

Тексеру алгоритмі есептеу күрделілігі, тексеру алгоритмі әдетте ықшам және жылдам болады.

$$P_V(m) = \begin{cases} Q(1), & zk - SHARK, \quad Grotth16 \\ Q(logm), & zk - STARK \\ Q(m), & Bulletpoofs \end{cases}$$

Дәлелдеме өлшемінің асимптотикалық бағалауы келесідей сипатталады.

$$|\pi| = \begin{cases} Q(1), & \text{қысқа дәлелдемелер} \\ Q(logm), & \text{орташа} \\ Q(m), & \text{үлкен дәлелдемелер} \end{cases}$$

Дәлелдемелер көлемінің ұлғаюы байланыс шығындарының өсуіне әкеледі.

Кесте 1 – Интерактивті емес нөлдік жария етілген дәлелдемелердің түрлері бойынша салыстырмалы кесте

Дәледемелердің түрлері	Setup моделі	$P_T(m)$	$P_V(m)$	Дәлелдеме өлшемі
$zk - SHARK$	CRS (сенімді)	$Q(m^2)$	$Q(1)$	Өте қысқа
$Grotth16$	CRS (сенімді)	$Q(m)$	$Q(1)$	Қысқа
$zk - STARK$	Орнатусыз	$Q(m\ logm)$	$Q(logm)$	Үлкен
$Bulletpoofs$	Орнатусыз	$Q(m\ logm)$	$Q(m)$	Орташа

Осы бөлімде теориялық асимтоталық бағалауларға сүйене отырып есептеу күрделілігі талданып, нәтиже көрсетеді.

Тізбектелген өңдеу платформасы параллелді есептеу мүмкіндіктері және іс жүзінде қолдануда тиімді әдістері ескеріліп қарастырылмаған. Соған қарамастан ұсынылған интерактивті емес нөлдік жария етілген дәлелдемелердің үлгілерінің өнімділігін салыстырмалы талдау үшін айтарлықтай теориялық базасын қамтамасыз етеді.

Нәтижелер мен талқылаулар

Зерттеуде интерактивті емес нөлдік дәлелдердің есептеуіш күрделілігі формальді түрде талданып, негізделген теориялық тұжырымдарға қол жеткізілді. Зерттеу әдістемесінде ұсынылған модель негізінде тексеру және дәлелдеу алгоритмдерінің есептеу күрделілігі асимтоталық түрде бағаланып, олардың арасындағы айырмашылық негізделді.

Зерттеу аясында интерактивті емес нөлдік жария етілген дәлелдемелердің есептеуіш күрделілігі полиномиалды уақыт моделінде формальді түрде талданып, бағаланды. Зерттеу барысында дәлелдеуші және тексеруші алгоритмдердің есептегіш күрделілігіне әсер ететін негізгі айнымалылар факторлық талдау арқылы анықталды.

Дәлдеушінің яғни дәлелдеуші алгоритмінің уақытша күрделілігі кіріс мәліметтерінің өлшемі (m) мен куәгердің ұзындығының $(|w|)$ көпмүшелік функциясымен шектелген, яғни интерактивті емес нөлдік жария етілген дәлелдеме жүйесінің дәлелдеуші алгоритмі полиномиалды уақытта жұмыс істейді.

$$\mathrm{C}_{\text{дәлелдеуші}} = poly\,(m) \cdot poly\,(|w|)$$

Дәлелдеушінің есептеуіш күрделілігі (m) мен $(|w|)$ параметрлеріне қатысты көпмүшелік шектеуде, атап айтқанда $poly\,(m), (|w|)$ функциясымен бағаланады. Бұл дәлелдеме құрастыру процесінің теориялық тұрғыдан тиімділігін және кіріс деректерінің көлеміне тәуелділіктің экспоненциалды түрде өспейтіндігін айқындайды.

Интерактивті емес нөлдік жария етілген дәлелдемелер NP толық есептер үшін анықталады, мұндағы куәгер $|w|$ кіріс өлшемі n – нен көпмүшелік тәелділікте шектелген.

$$|w| \leq \cdot poly\,(n\cdot)$$

Осы шарт дәлелдеуші алгоритмінің полиномалды уақыттық күрделілігінің *n*-ге тәуелді көпмүшелілік функциясымен шектелуіне жеткілікті.

$$\mathrm{C}_{\text{дәлелдеуші}} = poly\,(n\cdot)$$

Кіріс өлшемі m және дәлелдеме ұзындығы $|\pi|$ арқылы тексеру алгоритмінің күрделілігі өрнектеп жазуға болады.

$$\mathrm{C}_{\text{тексеруші}} = \cdot poly\,(m|\pi|)$$

Қолданбалы интерактивті емес нөлдік жария етілген дәлелдемелер хаттамаларында есептеу күрделілігі көбінесе логорифмдік немесе сызықтық өсу қарқынмен сипатталады.

π дәлелдеме үшін осы шартты орындауға болады.

$$|\pi| = \cdot \mathrm{O}\left(m^k\right),\ \ k \in N$$

Көпмүшелік шектеулілік қасиетін сақтайды, дәлелдеме ұзындығы кіріс деректерінің өлшеміне байланысты болғанда. Осы нәтиже кіріс өлшемі артқан сайын экспонециалды өсімнің болмауы коммуникативті күрделіліктің теориялық тұрғыдан тиімділігін айғақтайды.

Алынған нәтижелер тексеру және дәлелдеу алгоритмдерінің есептеу күрделілігі басқаша екенін көрсетеді. Дәлелдеу алгоритмнің есептеу жүктемесі салыстырмалы түрде жоғары, өйткені ол куәгердің мөлшеріне байланысты, ал алгортимді тексерушінің алгоритмі тек дәлелдеу мөлшеріне байланысты және айтарлықтай жеңіл болып табылады:

$$P_{Prove} \gg P_{Verify}$$

Бұл қасиет интерактивті емес нөлдік жария етілген дәлелдерді көп тексеруші жүйелер үшін пайдалы етеді.

Ресми талдау нәтижесінде өзара әрекеттесуге қатысты қатысы жоқ нөлдік жария етілген дәлелдемелердің барлық негізгі параметрлері көпмүшелік шегінде қалатыны анықталды:

$$P_{Prove}, P_{Verify}, |w|, |\pi| \leq poly\,(m)$$

Бұл нәтиже интерактивті емес нөлдік жария етілген дәлелдемелердің теориялық тұрғыдан тиімді және іс жүзінде қолданылатын криптографиялық механизмдер екенін көрсетеді.

Нәтижелер интерактивті емес нөлдік дәлелдемелерде дәлелдеуші мен тексеруші арасында есептеу жүктемесінің асимметриясы бар екенін көрсетті және бұл асимметрия жүйелерді масштабтау кезіндң маңызды артықшылық береді.

Қорытынды

Бұл мақалада көпмүшелік моделі аясында нөлдік қосындысы бар инерактивті емес нөлдік жария етілген дәлелдемелердің есептеу күрделілігі жан-жақты талданды. Зерттеу аясында инерактивті емес нөлдік жария етілген дәлелдемелердің схемаларының ресми моделі қарастырылып, дәлелденуші мен тексерушінің алгоритмдерінің есептеу шығындарына әсер ететін негізгі параметрлерді анықтайды.

Нәтижелер дәлелдеу алгоритмінің есептеу күрделілігі есептің өлшеміне және куәгердің өлшеміне байланысты екенін көрсетеді. Егер куәгердің мөлшері тапсырманың көлеміне қатысты көпмүшемен шектелсе, дәлелдемелерді құру процесі теориялық тұрғыдан тиімді. Бұл интерактивті емес нөлдік жария етілген дәлелдемелердің NP-класына қиын тапсырмалар үшін қолайлы екенін растайды.

Тексеруші алгоритмінің есептеу күрделілігі дәлелдеменің ұзындығына байланысты және көп жағдайда сызықтық немесе логарифмдік сипатта болатындығы анықталды. Бұл қасиет интерактивті емес нөлдік жария етілген дәлелдемелердің схемаларын көп тексерушісі бар бөлінген жүйелерде қолданысқа жарамдылығы, өнімділікті төмендетпей көлемді ұлғайтуды қолдану.

Талдау нәтижелері дәлелдеуші мен тексеру алгортимдерінің есептеуіш күрделілігінде айтарлықтай ассиметриялы екені анықталды. Дәлелдеушіге сәйкесінше жоғары есептеуіш күрделілікті арттырып, тексеру алгоритмі үйлесімді жүйенің жалпы өнімділігін арттыруға мүмкіндік береді. Бұл мүмкіндік электронды дауыс беру, аноноимді аутентификация құралдарында, блокчейн экожүйелерінде интерактивті емес нөлдік жария етілген дәлелдемелерін қолдануға негіз бола алады.

Жалпы алғанда жүргізілген ресми талдау интерактивті емес нөлдік қосынды дәлелдемелердің есептеу күрделілігі негізгі параметрлер бойынша көпмүшелік шегінде қалатынын көрсетті. Алынған нәтижелер қауіпсіз және масштабталатын криптографиялық хаттамаларды әзірлеудің теориялық негізі ретінде пайдалануы мүмкін. Нақты бағдарламалық жасақтаманы, аппараттық жеделдету әдістерін және эмпирикалық өнімдік көрсеткіштерін зерттеу болашық зерттеулердің өзекті бағыты болып табылады.

Әдебиеттер тізімі

1. How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design – Oded Goldreich, Silvio Micali & Avi Wigderson. Advances in Cryptology. – CRYPTO’86, Lecture Notes in Computer Science. – 1987. – Vol. 263. – P. 171-185. https://doi.org/10.1007/3-540-47721-7_11.
2. Fiat A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems / A. Fiat, A. Shamir // Advances in Cryptology - CRYPTO’86, LNCS 263, Springer. – 1987. https://doi.org/10.1007/3-540-47721-7_12.
3. Goldwasser S. The Knowledge Complexity of Interactive Proof Systems / S. Goldwasser, S. Micali, C. Rackoff // SIAM Journal on Computing. – 1989. – № 18(1). https://doi.org/10.1137/0218012.
4. Manuel B. Non-Interactive Zero-Knowledge and Its Applications / B. Manuel, P. Feldman, S. Micali // STOC ’88, ACM. – 1988. https://doi.org/10.1145/62212.62222.
5. Bellare M. Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols / M. Bellare, P. Rogaway // ACM CCS. – 1993. https://doi.org/10.1145/168588.168596.
6. Groth J. On the Size of Pairing-Based Non-interactive Arguments. Advances in Cryptology / J. Groth // EUROCRYPT. – 2016, LNCS 9665. https://doi.org/10.1007/978-3-662-49896-5_11.
7. Scalable, Transparent, and Post-Quantum Secure Computational Integrity / E. Ben-Sasson et al // IACR Cryptology ePrint Archive. – 2018. https://eprint.iacr.org/2018/046.
8. Bulletproofs: Short Proofs for Confidential Transactions and More / Benedikt Bünz et al // IEEE Symposium on Security and Privacy. – 2018. https://doi.org/10.1109/SP.2018.00020.
9. Quadratic Span Programs and Succinct NIZKs without PCPs / R. Gennaro et al // Advances in Cryptology – EUROCRYPT. – 2013. https://doi.org/10.1007/978-3-642-38348-9_35.

10. Micali S. Computationally Sound Proofs / S. Micali // SIAM Journal on Computing. – 2000. – № 30(4). https://doi.org/10.1137/S0097539795284959.
11. From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge / N. Bitansky et al // ITCS. – 2012. https://doi.org/10.1145/2090236.2090263.
12. Succinct Non-Interactive Arguments / A. Chiesa et al // IACR Cryptology ePrint Archive. – 2012. https://doi.org/10.1007/978-3-642-40041-4_9.
13. Adaptive Security for Interactive Proofs / R. Canetti et al // TCC. – 2002. https://doi.org/10.1007/978-3-642-40041-4_9.
14. Katz J. Introduction to Modern Cryptography / J. Katz, Y. Lindell // Chapman and Hall/CRC. – 2014. https://doi.org/10.1201/9781351133036.
15. Boneh D. A Graduate Course in Applied Cryptography / D. Boneh, V. Shoup // Draft textbook. – 2020. https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf.

Н.А. Модовов[1], Н.О. Мекебаев[1,2*], А.Б. Тлеубаева[3], О.М. Белгожа[2], І. Садыққан[2]
[1]Казахский национальный университет имени аль-Фараби,
050040, Казахстан, г. Алматы, пр. аль-Фараби, 71
[2]Казахский национальный женский педагогический университет,
050000, г. Алматы, Казахстан, ул. Гоголь 114 к1
[3]Шәкәрім университет,
071412, Казахстан, г. Семей, ул. Глинки, 20 А
*e-mail: nurbapa@gmail.com

АНАЛИЗ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ НЕИНТЕРАКТИВНЫХ ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Настоящая статья посвящена асимптотическому и формальному анализу вычислительной сложности не интерактивных доказательств с нулевым разглашением. Не интерактивные доказательства с нулевым разглашением позволяют доказывающей стороне подтвердить корректность некоторого утверждения проверяющей стороне без раскрытия какой-либо дополнительной информации и широко применяются в распределённых информационных системах. В ходе исследования схемы не интерактивных доказательств с нулевым разглашением рассматривались в модели общих исходных параметров (Common Reference String, CRS). При оценке вычислительной сложности в качестве основных параметров принимались временная сложность алгоритмов доказательства и проверки, размер свидетеля и длина доказательства. Эффективность алгоритмов анализировалась в рамках полиномиальной модели вычислений.
Показано, что вычислительная сложность алгоритма доказательства существенно зависит от размера свидетеля, тогда как сложность алгоритма проверки в основном определяется длиной доказательства. Кроме того, рассмотрены асимптотические оценки размера доказательств и их влияние на коммуникационные издержки. Полученные результаты могут быть использованы в качестве теоретической основы для сравнительного анализа не интерактивных доказательств с нулевым разглашением и разработки криптографических протоколов с высокой вычислительной эффективностью.

Ключевые слова: *не интерактивные доказательства с нулевым разглашением, криптография, алгоритмы доказательства и проверки, полиномиальное время, вычислительная сложность.*

N. Modovov[1], N. Mekebayev[1,2*], A. Tleubayeva[3], O. Belgozha[2], I. Sydykzhan[2]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,
050040, 71 Al-Farabi Ave., Almaty, Kazakhstan
[2]Kazakh National Women's Teacher Training University,
050000, 114 Gogol St., Almaty, Kazakhstan
[3]Shakarim University,
071412, 20A Glinka St., Semey, Kazakhstan
*e-mail: nurbapa@gmail.com

This paper is devoted to the asymptotic and formal analysis of the computational complexity of Non-Interactive Zero-Knowledge Proofs (NIZK). Non-interactive zero-knowledge proofs enable a prover to convince a verifier of the validity of a given statement without revealing any additional information and are widely applied in distributed information systems.

In this study, NIZK schemes are considered within the Common Reference String (CRS) model. The evaluation of computational complexity is based on the time complexity of the proving and verification algorithms, the witness size, and the proof length. Algorithmic efficiency is analyzed within the framework of the polynomial-time computational model.

The analysis shows that the computational complexity of the proving algorithm significantly depends on the witness size, whereas the complexity of the verification algorithm is mainly determined by the proof length. Additionally, asymptotic bounds on proof size and their impact on communication costs are examined. The obtained results provide a theoretical foundation for the comparative analysis of non-interactive zero-knowledge proofs and for the development of computationally efficient cryptographic protocols.

Key words: *non-interactive zero-knowledge proofs, cryptography, proving and verification algorithms, polynomial time, computational complexity.*

Авторлар туралы мәліметтер

Нурбол Алимбаевич Модовов – Ақпараттық қауіпсіздік жүйелері білім беру бағдарламасының 1 курс докторанты, әл-Фараби атындағы Қазақ ұлттық университетінің Алматы, Қазақстан; e-mail: modovov@gmail.com. ORCID: https://orcid.org/0009-0005-1642-9834.

Нурбапа Отанович Мекебаев* – PhD, Информатика кафедрасының қауымдастырылған профессоры, Қазақ ұлттық қыздар педагогикалық университеті, Алматы, Қазақстан; e-mail: nurbapa80@gmail.com. ORCID: https://orcid.org/0000-0002-9117-4369.

Аксауле Болатовна Тлеубаева – магистр, Шәкәрім универвитеті, Семей; e-mail: a.tleybaeva@shakarim.kz. ORCID: https://orchid.org/0000-0002-5121-5867.

Өркен Мұратханұлы Белгожа – магистр, Информатика кафедрасының оқытушысы, Қазақ ұлттық қыздар педагогикалық университеті, Алматы Қазақстан; e-mail: orkenbelkoja@gmail.com. ORCID: https://orcid.org/0009-0009-3231-1413.

Інжу Айдарқызы Сыдықжан – магистр, Қазақ ұлттық қыздар педагогикалық университеті, Алматы; e-mail: inzhusydykzhan@gmail.com. ORCID: https://orcid.org/0009-0005-8681-8835.

Сведения об авторах

Нурбол Алимбаевич Модовов – докторант 1 курса образовательной программы «Системы информационной безопасности», Al-Farabi Kazakh National University, Алматы, Казахстан; e-mail: modovov@gmail.com. ORCID: https://orcid.org/0009-0005-1642-9834.

Нурбапа Отанович Мекебаев* – PhD, ассоциированный профессор кафедры информатики, Казахский национальный женский педагогический университет, Алматы, Казахстан; e-mail: nurbapa80@gmail.com. ORCID: https://orcid.org/0000-0002-9117-4369.

Аксауле Болатовна Тлеубаева – магистр, Шәкәрім университет, Семей; e-mail: a.tleybaeva@shakarim.kz. ORCID: https://orchid.org/0000-0002-5121-5867.

Оркен Муратханович Белгожа – магистр, Казахский национальный женский педагогический университет, Алматы; e-mail: orkenbelkoja@gmail.com. ORCID: https://orcid.org/0009-0009-3231-1413.

Інжу Айдарқызы Сыдықжан – магистр, Казахский национальный женский педагогический университет, Алматы; e-mail: inzhusydykzhan@gmail.com. ORCID: https://orcid.org/0009-0005-8681-8835.

Information about the authors

Nurbol Modovov – 1st-year PhD doctoral student of the Information Security Systems educational program, Al-Farabi Kazakh National University, Almaty, Kazakhstan; e-mail: modovov@gmail.com. ORCID: https://orcid.org/0009-0005-1642-9834.

Nurbapa Mekebayev* – PhD, Associate Professor, Department of Informatics, Kazakh National Women's Teacher Training University, Almaty, Kazakhstan; e-mail: nurbapa80@gmail.com. ORCID: https://orcid.org/0000-0002-9117-4369.

Aksaule Tleubayeva – Master's degree holder, Shakarim University, Semey; e-mail: a.tleybaeva@shakarim.kz. ORCID: https://orchid.org/0000-0002-5121-5867.

Orken Belgozha – Master's degree holder, Lecturer of the Department of Computer Science, Kazakh National Women's Pedagogical University, Almaty, Kazakhstan; e-mail: orkenbelkoja@gmail.com. ORCID: https://orcid.org/0009-0009-3231-1413.

Inzhu Sydykzhan – Master's degree holder, Kazakh National Women's Teacher Training University, Almaty; e-mail: inzhusydykzhan@gmail.com. ORCID: https://orcid.org/0009-0005-8681-8835.

Редакцияға енуі 01.06.2026
Өңдеуден кейін түсуі 08.06.2026
Жариялауға қабылданды 17.06.2026