ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

2. M. J. Ablowitz and Z. H. Musslimani, “Интегрируемые нелокальные уравнения Шредингера,” Phys. Rev. Lett. 110, 064105 (2013).

ӘОЖ 004.056.5

ТОПТЫҚ ЭЦҚ: КЕЛІСІМДЕР МЕН ТРАНЗАКЦИЯЛАР ҚАУІПСІЗДІГІН АРТТЫРУ

Жанарбекұлы Алмаз
yaphets9705@hotmail.com
Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология мамандығының 1-курс магистранты
Ғылыми жетекшісі – Танирбергенов А. Ж.

Кіріспе

Топтық ЭЦҚ – бұл бірнеше қатысушыларға транзакцияны орындамас бұрын мақұлдауға мүмкіндік беретін технология. Бұл технология транзакциялардың қауіпсіздігін жақсарту үшін қолданылады, әсіресе криптовалюта саласында. Криптовалюта әлемінде транзакциялардың қауіпсіздігі маңызды фактор болып табылады, өйткені қатысушылардың қауіпсіздікке және алаяқтықтан қорғауға кепілдік беретін орталықтандырылған күші жоқ. Оның орнына транзакциялар орталықтандырылмаған желілер арқылы жүзеге асырылады, мұнда әрбір қатысушы әрбір транзакцияны тексеріп, оның дұрыстығын растай алады[1].

Алайда, бұған қарамастан, шабуылдаушылар алаяқтық операцияларды жасауға тырысатын жағдайлар болуы мүмкін. Бұл жағдайда мультипозиция көмекке келеді. Егер транзакция бірнеше қатысушының қолын талап етсе, онда алаяқ барлық қатысушылардың қолынсыз транзакцияны орындай алмайды, бұл мұндай транзакцияны қауіпсіз және қауіпсіз етеді. Осылайша, топтық ЭЦҚ пайдалану криптовалюта әлеміндегі транзакциялардың қауіпсіздігін арттырудағы маңызды қадам болып табылады. Бұл технологияны қаржы, құқықтану және басқалар сияқты басқа салалардағы транзакциялардың қауіпсіздігін қамтамасыз ету үшін пайдалануға болады[2].

Негізгі бөлім

Топтық ЭЦҚ – бұл бірнеше қатысушылардың электрондық құжатқа қол қою әдісі. Құжатқа қол қою үшін бір адамға сенудің орнына, топтық қолтаңба бірнеше адамнан қол қоюды талап етеді. Бұл қауіпсіздікті арттырады, өйткені әрбір қатысушы екіншісінің қолтаңбасын тексере алады, бұл құжатқа деген сенімділіктің жоғары деңгейін және ықтимал алаяқтық әрекеттерден қорғауды қамтамасыз етеді[3].

Кәдімгі криптографиялық қолтаңбада тек бір адам өзінің жеке кілтін пайдаланып транзакцияға қол қоя алады. Жағдайда топтық қолтаңба, бірнеше пайдаланушылар өздерінің жеке кілттерін пайдаланып транзакцияға бірлесіп қол қоя алады. Бұл қауіпсіз және сенімді транзакциялар жасауға мүмкіндік береді, өйткені бірнеше тараптардың қатысуы қажет, бұл алаяқтықты қиындатады және қаражатты жоғалту қаупін азайтады.

Топтық қолтаңба әдеттегі криптографиялық қолтаңбаларға қарағанда бірнеше артықшылықтарға ие[4]:

- Қауіпсіздік: топтық қолтаңба транзакциялардың қауіпсіздік деңгейін жоғарылатады, өйткені оларды жүзеге асыру үшін бірнеше қолтаңба қажет. Бұл дегеніміз, егер жүйеге қатысушылардың бірі хакерлік шабуылдың құрбаны болса немесе ережелерді әдейі бұзса да, қалған мүшелердің қатысуынсыз транзакция жасалмайды.

- Сенімділік: топтық қолтаңба транзакциялардың сенімділігін арттырады, өйткені бірнеше тараптың қатысуы қажет, бұл қол қою кезінде қателік қаупін азайтады және қаражаттың жоғалу мүмкіндігін азайтады.
- Ыңғайлылық: топтық қолтаңба – бұл әртүрлі параметрлер бойынша конфигурациялауға ыңғайлы технология, мысалы, транзакцияны жүргізу үшін қажетті қолтаңбалардың санын белгілеу, мүшелер тізімін анықтау және т. б.
- Бақылау: топтық қолтаңба жүйеге қатысушылардың әрекеттерін дәлірек бақылауға мүмкіндік береді, өйткені транзакцияны жүргізу үшін бірнеше Тараптың келісімі қажет. Бұл әсіресе көптеген қатысушылары бар компаниялар немесе ұйымдар үшін және қаржы ағындарын дәл бақылау мен басқару қажеттілігі үшін өте маңызды болуы мүмкін.
- Ашық: топтық қолтаңба жүйедегі әрекеттердің сенімділігін арттыра алады, өйткені барлық транзакциялар бірнеше мүшелерден өтеді, бұл ақпаратты жасыру және алаяқтық ықтималдығын азайтады.

Жалпы алғанда, топтық қолтаңба – бұл қаржылық ағындарды бақылау мен басқарудың сапасын жақсарту үшін әр түрлі салаларда қолдануға болатын қауіпсіз, сенімді және икемді технология.

Топтық қолтаңба алгоритмі бірнеше қадамдарды қамтиды[5]:

1. Әрбір қатысушы үшін жария және жеке кілттер жасау: әрбір қатысушы өзінің жария және жеке кілтін жасайды. Содан кейін жария кілттер транзакцияға қол қою үшін пайдаланылатын жария кілттер тобына жиналады.
2. Транзакцияны құру: бірнеше мүше қол қоюы керек транзакция жасалады.
3. Топтық қолтаңбаның мекен-жайын қалыптастыру: әр қатысушының жария кілттерін қолдана отырып, транзакцияны жіберу үшін пайдаланылатын топтық қолтаңбаның мекен-жайы жасалады.
4. Транзакцияға қол қою: әрбір қатысушы өзінің жеке кілтін пайдаланып транзакцияға қол қояды. Бұл бірнеше қолтаңбаны біреуіне қосуға мүмкіндік беретін арнайы алгоритмді қолданады топтық қолтаңба.
5. Топтық қолтаңбаны тексеру: барлық қатысушылар транзакцияға қол қойғаннан кейін, топтық қолтаңба дұрыстығы тексеріледі. Ол үшін барлық қолтаңбалардың дұрыстығын және топтық қолтаңбаның мекен-жайына сәйкес келетіндігін тексеретін арнайы алгоритм қолданылады.
6. Транзакцияны жүргізу: егер топтық қолтаңба дұрыс болса, транзакция жасалады және қаражат мақсатына аударылады. Егер топтық қолтаңба дұрыс болмаса, транзакция қабылданбайды.

Осылайша, топтық қолтаңбаның кеңейтілген алгоритмі ашық және жеке кілттерді құруды, топтық қолтаңбаны құруды, бірнеше қатысушылардың транзакцияға қол қоюын, топтық қолтаңбаны тексеруді және транзакцияны жүргізуді көздейді.

Топтық қолтаңба кез-келген жағдайда пайдалы болуы мүмкін, онда бірнеше мүше бірлесіп қол қойып, қандай-да бір транзакцияға немесе мәмілеге қол қоюы керек. Төменде топтық қолтаңба пайдалы болуы мүмкін кейбір мысалдар келтірілген:

- Криптоәмияндар: топтық қолтаңбаны бірнеше адам әмиянға кіре алатын және ақша аударымын мақұлдауы керек cryptocurrency әмияндарының қауіпсіздігін қамтамасыз ету үшін пайдалануға болады.
- Банктік шоттар: топтық қолтаңбаны банктік шоттардың қауіпсіздігін қамтамасыз ету үшін пайдалануға болады, мұнда бірнеше адам шотқа кіре алады және транзакцияны мақұлдауы керек.
- Компанияны басқару: топтық қолтаңба компанияны басқару үшін пайдаланылуы мүмкін, мұнда бірнеше адам компания атынан шешім қабылдауға құқылы.
- Нотариаттық қызметтер: топтық қолтаңба нотариаттық құжаттардың түпнұсқалығын қамтамасыз ету үшін пайдаланылуы мүмкін, мұнда бірнеше нотариустар құжатқа қол қоюы керек.

- Инвестициялар: топтық қолтаңбаны инвестициялардың қауіпсіздігін қамтамасыз ету үшін пайдалануға болады, мұнда бірнеше инвесторлар транзакцияны мақұлдауы керек.

Топтық қолтаңбаның бірқатар артықшылықтары болғанымен, кейбір кемшіліктері де бар:

- Пайдаланудың күрделілігі: топтық қолтаңбаны пайдалану қиын болуы мүмкін, әсіресе криптографияның техникалық аспектілерімен таныс емес пайдаланушылар үшін.
- Қатысушыларға тәуелділік: топтық қолтаңба жұмыс істеуі үшін барлық қатысушылар транзакцияға қол қоюы керек. Егер қатысушылардың бірі транзакцияға қол қоюдан бас тартса, бұл операцияның кешігуіне немесе тоқтатылуына әкелуі мүмкін.
- Жоғары төлемдер: топтық қолтаңбаны пайдалану қосымша төлемдер мен шығындарға байланысты болуы мүмкін, бұл операцияның экономикалық тиімділігіне әсер етуі мүмкін.
- Әмиянға қол жетімділікті жоғалту қаупі: егер қатысушылардың бірі әмиянға қол жеткізе алмаса, бұл транзакция жасау мүмкін кстігіне немесе қаражаттың жоғалуына әкелуі мүмкін.
- Орталықтандыру қаупі: топтық қолтаңбаны пайдалану биліктің орталықтандырылуына әкелуі мүмкін, өйткені барлық қатысушылар бір жерде тіркелуі керек, бұл қауіпсіздік осалдығына әкелуі мүмкін.

Жалпы алғанда, топтық қолтаңбада бірқатар шектеулер бар, бірақ бұл қауіпсіздіктің жоғарылауы қажет болған жағдайда және бірнеше мүше транзакцияға бірлесіп қол қоюы керек болған жағдайда пайдалы болуы мүмкін.

Қорытынды.

Топтық қолтаңба – бұл бірнеше қолтаңбаны қажет ететін транзакциялар мен мәмілелердің қауіпсіздік деңгейін арттыруға мүмкіндік беретін құрал. Топтық қолтаңба қаржы және мәмілелер саласындағы қауіпсіздікті арттырудың қуатты құралы болып табылады, әсіресе транзакцияны растау үшін бірнеше мүше қажет болған жағдайда. Оны пайдалану транзакцияға қол қою және бекіту процесін орталықтандырылмаған етуге, ашықтықты арттыруға және қатысушылар арасында жауапкершілік пен бақылаудың біркелкі бөлінуін қамтамасыз етуге мүмкіндік береді.

Алайда, кез-келген құрал сияқты, топтық қолтаңбаның да кемшіліктері жоқ емес. Оны пайдалану қосымша төлемдер мен шығындарға байланысты болуы мүмкін және барлық қатысушылардан криптографияның техникалық аспектілері туралы білімді талап етеді, бұл қиындықтар тудыруы мүмкін. Сонымен қатар, топтық қолтаңба қатысушыларға байланысты, егер қатысушылардың бірі транзакцияға қол қоюдан бас тартса, операцияның кешігуіне немесе тоқтатылуына әкелуі мүмкін.

Жалпы алғанда, топтық қолтаңба қаржы, үкімет, денсаулық сақтау және т.б. қоса алғанда, әртүрлі салаларда қауіпсіздік пен сенімділікті қамтамасыз етудің пайдалы құралы болып табылады. топтық қолтаңба, оның артықшылықтары мен кемшіліктерін бағалау, тәуекелдерді ескеру және транзакциялардың қауіпсіздігі мен тиімділігін қамтамасыз ету үшін тиісті шараларды қабылдау маңызды.

Қолданылған әдебиеттер

1. Rivest R., Shamir A., Adleman A. A method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of the ACM. — 1978. —V. 21. — N. 2.
2. V.S. Miller. Use of elliptic curves in cryptography, Cryptology, CRYPTO’85, LNCS 218, 1985.
3. Гурьянов Д.Ю., Дернова Е.С., Избаш В.И., Молдовян Д.Н. Алгоритмы электронной цифровой подписи на основе сложности извлечения корней в конечных группах известного порядка // Информационно-управляющие системы. 2008. № 5.

4. Молдовян А.А., Молдовян Н.А. Новые алгоритмы и протоколы для аутентификации информации в АСУ // Автоматика и телемеханика. 2008. № 7.
5. Молдовян Д.Н. Новый механизм формирования подписи в схемах ЭЦП, основанных на сложности дискретного логарифмирования и факторизации. // Вопросы защиты информации. 2005. №4.

УДК 519.62

СТАЦИОНАРНОЕ РЕШЕНИЕ ОДНОМЕРНОГО УРАВНЕНИЯ СЕН-ВЕНАНА

Жантлеуова Асель Канатовна
zhantleuova.asel@mail.ru
Магистрант 2-го курса Казахского национального педагогического университета имени Абая, Алматы, Казахстан
Научные руководители — д.ф.-м.н., профессор Бердышев А. С., доктор PhD, ст.преподаватель Касенов С.Е.

Уравнения Сен-Венана (также известное как система уравнений Сен-Венана) — это дифференциальные уравнения, описывающие течение мелкой воды, часто используемые для моделирования различных явлений в механике жидкости, включая течение рек, озер и прибрежных районов. Решение уравнения Сен-Венана имеет важное практическое применение в гидрологии и гидравлике.

Нелинейные уравнения Сен-Венана с наклоном и трением задаются следующей системой [1]:

$$\frac{\partial H(t,x)}{\partial t} + \frac{\partial (H(t,x)V(t,x))}{\partial x} = 0, \quad (1)$$

$$\frac{\partial V(t,x)}{\partial t} + \frac{\partial}{\partial x}\left(\frac{V^2(t,x)}{2} + gH(t,x)\right) + \left(\frac{kV^2(t,x)}{H(t,x)} - gC(x)\right) = 0, \quad (2)$$

где $H(t,x)$ – глубина воды; $V(t,x)$ – горизонтальная скорость воды. Наклон $C(\cdot) \in C^2([0,L])$ определяется $C(x) = -\frac{dB}{dx}$ с высотой дна $B(x)$, которая, следовательно, должна быть C^3 (не менее трех раз непрерывно дифференцируемой), g - постоянное ускорение силы тяжести и k - постоянный коэффициент трения.

Из (1) и (2) следует, что для стационарного решения $H_0(x)$ и $V_0(x)$ система примет следующий вид:

$$H_0(x)V_0(x) = Q, \quad (3)$$

$$V_0'(x) = \frac{V_0^2(x)\left[\frac{kV_0^3(x)}{Q} - gC(x)\right]}{gQ - V_0^3(x)} \quad (4)$$

Мы рассматриваем случай, соответствующий физическому стационарному состоянию, т. е. в стационарном состоянии поток жидкости должен непрерывно и