ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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 имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

$$\Psi_{Ua+}(k,\theta,x_1) = \Psi_0(k,\theta,x_1) + \sum_{n=1}^{\infty}\prod_{k=1}^{n}\int \frac{q_{Ua}(x_{k+1})e^{ik|x_k - x_{k+1}|}}{|x_k - x_{k+1}|}\Psi_0(k,\theta,x_{n+1})dx_2 \dots dx_{n+1} \quad (7)$$

Теорема 4. : Амплитуды функций Ψ_{Ua_+} и Ψ_+ могут быть вычислены как:

$$A_{Ua}(k,\theta',\theta) = e^{ik(\theta-\theta',a)}A(k,\theta',\theta)$$

Доказательство: Из теоремы (2)

$$A_{Ua+}(k,\theta',\theta) = -(1/(4\pi))\int q_{Ua}(x_1)\Psi_0(k,\theta,x_1)\Psi_{Ua}(k,-\theta',x_1)dx_1 \quad (8)$$

Из теоремы (3)

$$A_{Ua+}(k,\theta',\theta) = -(1/(4\pi))\int q_{Ua}(x_1)\Psi_0(k,\theta,x)[\Psi_0(k,-\theta',x_1) + \sum_{n=1}^{\infty}\prod_{k=1}^{n}\int \frac{q_{Ua}(x_{k+1})e^{ik|x_k - x_{k+1}|}}{|x_k - x_{k+1}|}\Psi_0(k,-\theta',x_{n+1})]dx_2 \dots dx_{n+1}dx_1$$

$$A_{Ua+}(k,\theta',\theta) = e^{ik(\theta'-\theta)}A(k,U'\theta',U'\theta)$$

Раскрытие инвариантности дискретности собственных значений в уравнениях Шрёдингера: ключевые аспекты и практические приложения

В данном исследовании раскрывается значительная связь, касающаяся инвариантности дискретности собственных значений для семейства потенциалов, полученных путем линейных преобразований переменных. Простота этих преобразований показывает, что многие достижения, полученные с использованием пар Лакса, являются внутренними свойствами, возникающими в результате линейных преобразований переменных в уравнениях Шрёдингера.

Для анализа и оптимального использования сейсмических данных.

Для анализа и оптимального использования данных ультразвукового сканирования.

Для анализа и оптимального использования данных электромагнитного сканирования.

Для анализа и оптимального использования данных о нелинейных колебаниях сканирования.

Список использованных источников

1. E. Schrödinger, "Quantisierung als Eigenwertproblem (Erste Mitteilung)," Annalen der Physik, Vol. 384(79), pp. 361-376, 1926.
2. E. Schrödinger, "Quantisierung als Eigenwertproblem (Zweite Mitteilung)," Annalen der Physik, Vol. 384(79), pp. 489-527, 1926.
3. C. S. Gardner, J. M. Greene, M. D. kruskal, R. M. Miura, "Method for Solving the korteweg-deVries Equation," Physical Review Letters, Vol. 19, pp. 1095-1097, 1967.
R. G. Newton, "Inverse scattering Three dimensions," Journal of Mathematical Physics, Vol. 21, pp. 1698-1715, 1980.

ӘОЖ 004.056.5

ПРАКТИКАЛЫҚ ТОПТЫҚ ҚОЛ ҚОЮ ХАТТАМАЛАРЫН ҚҰРУ ЖӘНЕ ӘЗІРЛЕУ ӘДІСТЕРІ

Жанарбекұлы Алмаз
yaphets9705@gmail.com
Л Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология мамандығының 2-курс магистранты
Ғылыми жетекшісі – А. Ж. Танирбергенов

Аннотация

Бұл мақалада топтық қол қоюдың практикалық хаттамаларын құру және әзірлеу әдістері қарастырылады. Топтық қол қою хаттамалары электрондық құжаттар мен хабарламалардың қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады, бұл бірнеше қатысушыларға деректерге ұжымдық қол қоюға мүмкіндік береді. Біз осындай хаттамаларды әзірлеудің әртүрлі тәсілдерін,

соның ішінде криптографиялық алгоритмдер мен математикалық конструкцияларға негізделген әдістерді сипаттаймыз. Қауіпсіздік пен тиімділіктің жоғары деңгейін қамтамасыз ететін хаттамаларды қоса алғанда, классикалық әдістер де, жаңа тәсілдер де талқыланады. Біздің мақаламыз криптография және ақпараттық қауіпсіздік саласындағы зерттеушілер мен тәжірибешілерге топтық қол қою хаттамаларын әзірлеудің негізгі принциптері мен әдістерін түсінуге, сондай-ақ нақты қолданбалы тапсырмалар үшін ең қолайлы тәсілді таңдауға көмектеседі.

Кіріспе

Қазіргі ақпараттық қоғамда электрондық құжаттар мен хабарламалар ақпарат алмасуда шешуші рөл атқарады. Дегенмен, олардың тұтастығы мен шынайылығын қамтамасыз ету маңызды, әсіресе құпия деректер мен маңызды құжаттарды тарату контекстінде. Бұл тұрғыда топтық қол қою хаттамалары электрондық коммуникациялардың қауіпсіздігін қамтамасыз етудің маңызды құралына айналуда. Топтық қол қою хаттамалары бірнеше қатысушыларға электрондық құжаттарға немесе хабарламаларға ұжымдық қол қоюға мүмкіндік береді, осылайша деректердің тұтастығы мен түпнұсқалығын қамтамасыз етеді. Бұл әдіс жеке қолтаңбамен салыстырғанда айтарлықтай артықшылықтарға ие, өйткені ол әр топ мүшесінен жеке қолтаңбаны қажет етпейді.

Дегенмен, тиімді және қауіпсіз топтық қол қою хаттамаларын әзірлеу криптографияның, математиканың және ақпараттық қауіпсіздіктің әртүрлі аспектілерін ескеруді талап ететін тривиальды емес тапсырма болып табылады. Бұл мақалада біз топтық қол қоюдың практикалық хаттамаларын құру және әзірлеу әдістерін қарастырамыз, олардың негізгі принциптері мен әдістерін талқылаймыз және осы саладағы қолданыстағы тәсілдер мен жаңа әзірлемелерге шолу жасаймыз.

Негізгі бөлім

Топтық қол қоюдың практикалық хаттамаларын құрудың негізгі әдістері құжаттарға немесе хабарламаларға ұжымдық қол қою мүмкіндігін қамтамасыз ететін әртүрлі алгоритмдер мен схемаларды қамтиды. Бірнеше негізгі тәсілдерді қарастырыңыз:

Хэшке негізделген схемалар: бұл схемалар бірнеше мүшелердің қолтаңбаларын бір топтық қолтаңбаға біріктіру үшін хэш функцияларын пайдаланады. Мұндай схеманың бір мысалы-Меркл-Дамгард схемасы, мұнда хэш функциялары оларды біріктірмес бұрын әр қолтаңбаға қолданылады. Бұл тәсіл жоғары тиімділік пен қауіпсіздікті қамтамасыз етеді.

Эллиптикалық қисықтарға негізделген схемалар: бұл схемалар топтық қолтаңбаларды жасау үшін эллиптикалық қисықтардың математикалық қасиеттерін пайдаланады. Эллиптикалық қисықтарға негізделген хаттамалар шабуылға жоғары төзімділікке ие және оларды іс жүзінде тиімді жүзеге асыруға болады.

Біріктірілген әдістер: кейбір топтық қол қою схемалары қауіпсіздік пен өнімділік арасындағы оңтайлы тепе-теңдікке қол жеткізу үшін әртүрлі алгоритмдер мен әдістерді біріктіреді. Мысалы, қолтаңбаларды біріктіру үшін хэш-функцияға негізделген схемаларды қолдану, содан кейін соңғы топтық қолтаңбаны жасау үшін эллиптикалық қисық сызбаларды қолдану.

Бұл әдістердің әрқайсысының артықшылықтары мен кемшіліктері бар және белгілі бір тәсілді таңдау қауіпсіздік талаптарына, өнімділікке және белгілі бір қолданбаның басқа факторларына

байланысты. Сондай-ақ криптографиялық қауіпсіздік стандарттарын және қолданыстағы инфрақұрылыммен біріктіру мүмкіндігін ескеру маңызды.

Топтық қолтаңбалар бірнеше мүшелерден немесе топтан аутентификация қажет болған жағдайда электрондық құжаттар мен хабарламалардың қауіпсіздігі мен тұтастығын қамтамасыз етуде маңызды рөл атқарады. Міне, олардың маңызды болуының бірнеше себептері:

Деректердің аутентификациясы және тұтастығы: топтық қолтаңбалар бірнеше мүшеге құжаттың немесе хабарламаның түпнұсқалығы мен тұтастығын растайтын аутентификацияға мүмкіндік береді. Бұл әсіресе қаржылық транзакциялар немесе құпия ақпаратпен алмасу сияқты электрондық деректерге қауіпсіздік пен сенімділікті қамтамасыз ету қажет салаларда өте маңызды.

Жауапкершілік және бас тартпау: топтық қолтаңбалар қол қою жауапкершілігін бірнеше мүшелер арасында бөлуге мүмкіндік береді. Бұл қол қоюдан біржақты бас тарту немесе қол қойылғаннан кейін деректерді өзгерту мүмкіндігінен қорғаудың қосымша қабатын қамтамасыз етеді.

Тәуекелдерді азайту: топтық қолтаңбаларды пайдалану орталықтандырылған кілттерді басқаруға немесе жеке мүшеге сенуге байланысты тәуекелдерді азайтады. Қатысушылар арасындағы жауапкершілікті бөлу жүйені шабуылдарға немесе бұзылуларға төзімді етеді.

Заңды сәйкестік: заң немесе мемлекеттік ұйымдар сияқты кейбір салаларда құжаттар мен хабарламаларға қол қоюға заңнамалық талаптар бар. Топтық қолтаңбалар ұжымдық мақұлдау мен аутентификация механизмін ұсыну арқылы осы талаптарды орындауға көмектеседі.

Топтық қолтаңбалар электрондық құжаттар мен хабарламалардың қауіпсіздігі мен тұтастығын қамтамасыз етуде маңызды рөл атқарады. Олар жіберушіні аутентификациялауға, деректердің тұтастығын қамтамасыз етуге және рұқсатсыз кіру тәуекелдерін азайтуға мүмкіндік береді.Зерттеу барысында кеңейтілген функционалдығы және жоғары қауіпсіздік деңгейі бар топтық қол қоюдың инновациялық хаттамалары әзірленді. Бұл хаттамалар қаржы институттары, мемлекеттік ұйымдар және басқалар сияқты әртүрлі салаларда қауіпсіздікті қамтамасыз етудің маңызды құралы болып табылады.Топтық қолтаңбаларды одан әрі зерттеу және дамыту тиімдірек хаттамалар жасауды, сондай-ақ оларды заманауи технологиялық және құқықтық талаптарға бейімдеуді қамтуы мүмкін. Бұл электрондық жүйелердің қауіпсіздік деңгейін арттыруға және олардың заманауи стандарттар мен нормативтерге сәйкестігін қамтамасыз етуге мүмкіндік береді.

Бұл зерттеудің нәтижелері ақпараттық жүйелердің қауіпсіздігін жақсартуға және электрондық коммуникацияларға деген сенімді арттыруға ықпал ете отырып, экономиканың және жалпы қоғамның әртүрлі секторлары үшін пайдалы болуы мүмкін.

Теориялық тұжырымдардан басқа, зерттеудің практикалық маңызы да бар, өйткені әзірленген хаттамаларды деректердің қауіпсіздігі мен аутентификациясын қамтамасыз ету үшін нақты жүйелерде пайдалануға болады.

Қорытынды

Жұмыста электрондық құжаттар мен хабарламалардың қауіпсіздігі мен тұтастығын қамтамасыз етуде маңызды рөл атқаратын топтық қол қоюдың практикалық хаттамаларын құру және әзірлеу әдістері қарастырылды. Топтық қолтаңбалардың маңыздылығы олардың аутентификацияны, деректердің тұтастығын, жауапкершілікті бөлуді және тәуекелдерді азайтуды және сәйкестікті қамтамасыз ету қабілетінде.

Әзірленген топтық қолтаңба хаттамалары кеңейтілген функционалдылыққа және қауіпсіздіктің жоғары деңгейіне ие инновациялық әдістер болып табылады. Оларды практикалық қолдану қаржылық транзакциялар, Құқықтану, мемлекеттік ұйымдар және т.б. сияқты әртүрлі салаларда қауіпсіздікті жақсартуға ықпал етуі мүмкін.

Топтық қолтаңбаларды одан әрі дамыту және зерттеу тиімдірек және сенімді хаттамаларды құруды, сондай-ақ қолданыстағы әдістерді жаңа технологиялық және құқықтық талаптарға бейімдеуді қамтуы мүмкін. Бұл электрондық жүйелердің қауіпсіздігін жақсартуға және олардың заманауи стандарттар мен нормативтерге сәйкестігін қамтамасыз етуге мүмкіндік береді.

Қолданылған әдебиеттер тізімі:

1. Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
2. Коблиц, Н. (1994). A Course in Number Theory and Cryptography. Springer-Verlag.
3. Washington, L. C. (2008). Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC.
4. Stinson, D. R. (2005). Cryptography: Theory and Practice. Chapman and Hall/CRC.
5. Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.

УДК 004.4

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Жолдубаева Диана Турлановна
diana-328@mail.ru
Магистрант 2 курса Евразийский национальный
университет имени Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Сулейменов К.М.

Аннотация

Данная статья исследует эффективные методы реализации цифровой подписи на основе эллиптической кривой. Эллиптические кривые представляют собой мощный математический инструмент, используемый в криптографии для обеспечения безопасности передачи данных. В статье рассматриваются основные принципы работы с эллиптическими кривыми в контексте цифровой подписи, а также предлагаются новые методы оптимизации для повышения скорости и безопасности подписи. Результаты исследования могут быть полезны для разработчиков криптографических систем, стремящихся к оптимальной и надежной реализации цифровой подписи на основе эллиптической кривой.

Введение

Цифровая подпись является одним из важнейших инструментов в современной криптографии, обеспечивающим аутентификацию и целостность данных. Одним из наиболее эффективных методов реализации цифровой подписи является использование эллиптических кривых. Эллиптические кривые обладают высоким уровнем безопасности при сравнительно небольшой длине ключа, что делает их привлекательным выбором для многих криптографических протоколов.

Определение эллиптической кривой

Эллиптическая кривая определяется уравнением вида: