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

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2023

Қорғаныс түрлендірулерінің алгебралық алгоритмдерінің басты артықшылықтарының бірі-олар дұрыс іске асырылған кезде қауіпсіздіктің жоғары деңгейіне ие. Сонымен қатар, алгоритмдерді аппараттық құралдармен жеделдетуге болады, бұл үлкен көлемдегі деректерді жылдам өңдеуге мүмкіндік береді. Бұл алгоритмдердің барлығы ақпаратты шифрлау және шифрын ашу үшін үлкен санды операциялар, Галуа түрлендірулері, XOR операциялары және т.б. сияқты математикалық функцияларды пайдаланады. Олар деректерді тек кілті бар адам ғана деректердің шифрын ашып, ақпаратқа қол жеткізе алатындай етіп түрлендіру арқылы ақпаратты қорғауды қамтамасыз етеді.

Қорғаныс түрлендіру алгоритмдерінің беріктігін оларды бұзу үшін қолдануға болатын шабуылдар арқылы бағалауға болады. Ең көп таралған шабуылдардың бірі-шабуылдаушы дұрыс комбинацияны тапқанға дейін барлық мүмкін кілттер тіркесімін немесе басқа алгоритм параметрлерін сұрыптайтын шамадан тыс шабуыл.

Мұндай шабуылдарға қорғаныс түрлендіру алгоритмдерінің беріктігін арттыру үшін S-блоктары, элементтерді ауыстыру, бағандарды араластыру және жолдарды ауыстыру сияқты қосымша түрлендірулер жиі қолданылады. Алайда, түрлендірулердің тіркесіміне негізделген алгоритмдерді түсіну қиын болуы мүмкін және оларды шамадан тыс шабуылдармен бұзуға болады.

Алайда, ақпаратты қорғау алгоритмдерін іске асыру кезінде бірқатар шектеулерді ескеру қажет. Біріншіден, қауіпсіздікті қамтамасыз ету үшін кілттер мен алгоритмдерді дұрыс таңдау керек. Екіншіден, кілттерді сақтау және беру қауіпсіздігін қамтамасыз ету қажет. Үшіншіден, мүмкін шабуылдарды қиындату үшін жеткілікті күрделі алгоритмдер мен кілттерді қолдану қажет.

Қорыта айтқанда қорғаныс түрлендірулерінің алгебралық алгоритмдері ақпараттың қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Олар цифрлық құжаттарды шифрлау және қол қою, деректердің құпиялылығы мен тұтастығын қамтамасыз ету үшін қолданылады. Мұндай алгоритмдердің мысалдары RSA, AES және Blowfish болып табылады. Алайда, ақпаратты қорғау алгоритмдерін іске асыру кезінде бірқатар шектеулерді ескеру және деректердің қауіпсіздігін қамтамасыз ету үшін дұрыс тәжірибелерді сақтау қажет.

Қолданылған әдебиеттер тізімі:

1. Иванов М. А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях.- М.: НИЯУ МИФИ, 2012.

2. Молдовян Д.Н., Молдовян Н.А. Введение в теоретические основы криптоситем с открытым ключом.-- СПб.: Изд–во ГУМРФ им. адмирала С.О. Макарова, 2016.

3. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. –М.: Юрайт, 2016.

ӘОЖ 004.056

АШЫҚ КІЛТТІ КРИПТОГРАФИЯЛЫҚ ЖҮЙЕГЕ НЕЙРОНДЫҚ ЖЕЛІЛЕРДІҢ ҚОЛДАНЫЛУЫ

Асқарқызы Нұргүл

askarkyzyng@gmail.com

Л.Н.Гумилев атындағы ЕҰУ «6В06105- Математикалық және компьютерлік модельдеу» мамандығының 4 курс студенті, Астана, Қазақстан

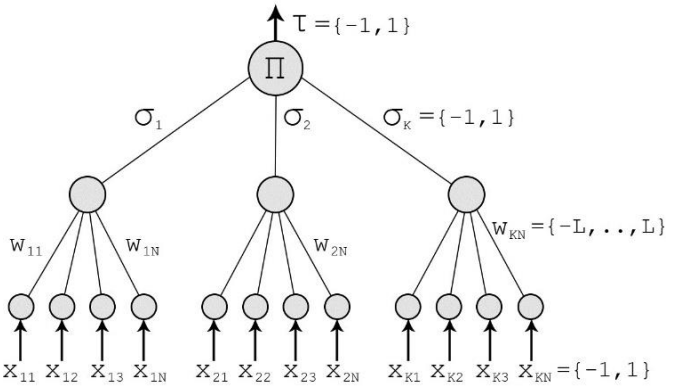
Ғылыми жетекшісі- К.М. Сулейменов

Жасанды нейрондық желі - адамның миындағы биологиялық нейрондардың жұмыс жасауының математикалық моделі. Негізгі идеясы 1943 жылы американдық нейропсихолог Уоррон Мак-Келлок және американдық математик Уалтер Питспен ұсынылған болатын. 1958 жылы Фрэнк Розенблатт қазіргі кездегі нейрондық желілердің ең қарапайым нұсқасы болып есептелінетін, “перцептрон” деп аталатын нейрондық желіні ойлап тапты. Қазіргі таңға дейін әлі де қызу талқыға салынып келе жатырған жасанды нейрондық желі, машиналық оқытудың бір бөлігі ретінде есептеліп, биология, медицина, математика, физика және т.б. салаларда кеңінен қолданылуда. Сонымен қатар криптографияға да мәліметтерді қорғау мақсатында енгізілуде.

Криптографияға мәліметтерді қорғау мақсатында жасанды желілердің қолданылуы нейрокриптография деп аталатын жаңа криптография бөлімін туғызды.Бұл саладағы ең алғашқы қарастырылған мәселердің бірі- нейрондық желілер көмегімен құпия кілтті генерациялау болды. Классикалық криптографияда шифрлеу жүйелері екіге бөлінеді: симмертриялы және асимметриялы (немесе ашық кілтті) криптографиялық жүйе. Симметриялы криптографиялық жүйеге мәліметті шифрлеу және дешифрлеу үшін бір кілт қолданылатын жүйелер жатқызылады. Ал екінші түрі шифрлеу үшін ашық кілтті және дешифрлеу кезінде құпия кілтті қолданатын жүйелерді қамтиды. Алғашқы жүйе уақыт жағынан эффективтілігі жоғары болғанымен, кілт қауіпсіз емес байланыс каналынан өтетін болғандықтан, ашық кілтті криптографиялық жүйелер қолданыста жиі таралған. Ұсынылған нейрондық желі көмегімен кілт алмастыру нейрондар синапстарының салмақтары синхронизациялануы көмегімен жүзеге асады.

Кілтпен алмасатын екі жақты бір кіріс және шығыс қабаттары және бір жасырын қабаттан тұратын жасанды нейрондық желілер деп қарастырайық. Жасырын қабаты K тәуелсіз перцептрондардан тұрады, ал одан кейінгі шығыс қабаты K жасырын қабатының жұптылығын тексереді. Әрбір K перцептроны N кіріс нейрондардан $x_{k,n}$ және сәйкесінше синапс салмақтарын $w_{k,n}$ қамтиды. Мұндағы $x_{k,n} \in \{-1,1\}$, $w_{k,n} \in \{-L, L\}$, $k = \overline{1,K}$, $n = \overline{1,N}$. L – синапстың басымдылығын білдіретін дискректті шама.

Қарастырылған структурадағы нейрондық көп қабатты нейрондық желіні ағаш жұптылығы машинасы (tree parity machine) деп аталады.



Сурет 1. Ағаш жұптылығы машинасы (tree parity machine)

Әрбір K перцептрон үшін шығыс мәні келесідей анықталады:

$$\sigma_k = sign\left(\sum_{n=1}^{N} x_{k,n} w_{k,n}\right), \quad (1)$$

Мұндағы

$\sigma_k - k$-сыншы перцертронның шығыс мәні.

sign(x) –перцептрон үшін активация функциясы ретінде қолданылып тұрған таңба функциясы

$$sign(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases}, \quad (2)$$

Нейрондық желінің шығыс мәні барлық K перцептрондардың жұптығы ретінде есептеледі

$$\tau = \prod_{k=1}^{K} \sigma_k = \prod_{k=1}^{K} sign\left(\sum_{n=1}^{N} x_{k,n} w_{k,n}\right) \quad (3)$$

$\tau -$ нейрондық желінің қорытынды шығыс мәні

Екі нейрондық желілердің синаптикалық салмақтары синхронизациялануы келесі алгоритммен жүзеге асады. Кілтпен алмасатын екі жақты Алиса және Боб деп атайық.

1. Екі жақта,тек өздеріне белгілі болатындай рандомды түрде салмақ мәндерін $w_{k,n}$ таңдап алады.
2. Кіріс мәндер $x_{k,n}$ ашық кілт есебінде екі жаққа да бірдей рандомды түрде генерацияланады.
3. Егер нейрондық желілердің шығыс мәні τ бір бірімен тең болса ($\tau_A = \tau_B$) онда синхроницазиялаудың келесі кезеңіне өтеді, ал тең болмаса қайтадан екінші қадамға оралады
4. Шығыс мәндері тең болған кезде нейрондық желілерді оқыту жүреді
5. Машиналар оқытылғаннан кейін, салмақтары тексеріледі. Егер бірдей болған жағдайда, екі жаққа да белгілі құпия кілтті аламыз, ал тең болмаса қайта екінші қадамға өтеміз

Нейрондық желілерді оқыту үшін “оқытушысыз оқытудың”(unsupervised learning) әдістері қолданылады. Мысалы, Хебб оқытуы. Хебб оқытуы, 1949 жылы Дональд Хебб ұсынған Хебб ережесі негізінде құрылған. Хебб ережесінде “ Егер А жасушасының аксоны В жасушанына жеткілікті түрде жақын тұрса, және бірнеше рет немесе үнемі онымен байланысса, онда екі жасушаның біреуінде немесе екеуінде де бір бірімен байланысу кезінде тиімділігінің артуы байқалады”

$$w' = w + \Delta w \quad (4)$$

$$\Delta w = \eta x y \quad (5)$$

(4) тендеуі Хебб оқытуы теңдеуінің жалпылама түрі. Мұндағы,

$w -$ екі нейронның (пресинапстық және постсинапстық) арасындағы байланыс(синапс) салмағы

$w' -$ келесі итарициядағы екі нейронның арасындағы байланыс

$\Delta w -$ салмақтың өзгерісін білдіретін өсімше

$\eta -$ оқыту жылдамдығын білдіретін, оң мәнді коэффициент

$x -$ пресинапстық нейронның мәні

$y -$ пост синапстық нейрон мәні

(5) – Әрекет өнімінің ережесі. Теңдеу синапстың корреляциялық сипатын көрсетеді.

Жалпылама теңдеуді қарастырылып жатырған нейрондық желі үшін сипаттайық. Қарастырылып жатырған нейрондық желілер оқытылуы екі нейрондық желінің шығыс мәндері тең болса ғана жүргізіледі. Сондықтан, келесі функцияны енгізейік:

$$\theta(a,b) = \begin{cases} 1, & a = b \\ 0, & a \neq b \end{cases} \quad (6)$$

Сондай-ақ, нейрондық желілер арасындағы қауіпсіздікті арттыру үшін $\tau = \sigma_k$ шартын қанағаттандыратын k-шы перцепрондар үшін салмақтар жаңартылсын.

Δw-дегі η мәні үшін

$$\eta = \theta(\sigma_k, \tau)\theta(\tau_A, \tau_B) \quad (7)$$

деп алайық, мұндағы τ_A, τ_B сәйкесінше, Алиса мен Бобтың шығыс мәндері.

Барлық параметрлерді орнына қойсақ,

$$w_{k,n}{}' = w_{k,n} + \theta(\sigma_k, \tau)\theta(\tau_A, \tau_B)x_{k,n}\sigma \quad (8)$$

$w_{k,n} \in \{-L, L\}$ болғандықтан, келесі функцияны енгізейік:

$$g(w) = \begin{cases} sign(w)L, & |w| > L \\ w, & |w| \leq L \end{cases} \quad (9)$$

(8) теңдеуге (9) функциясын қолдансақ,

$$w_{k,n}{}' = g\left(w_{k,n} + \theta(\sigma_k, \tau)\theta(\tau_A, \tau_B)x_{k,n}\sigma\right) \quad (10)$$

Алынған (10) теңдеумен нейрондық желілерді жаттықтырамыз.

Жұмыс кезінде Хебб оқыту теңдеуінен басқа, Анти-Хебб (11) және Кейзейсоқ қадамдар(12) оқыту әдістері қарастырылды.

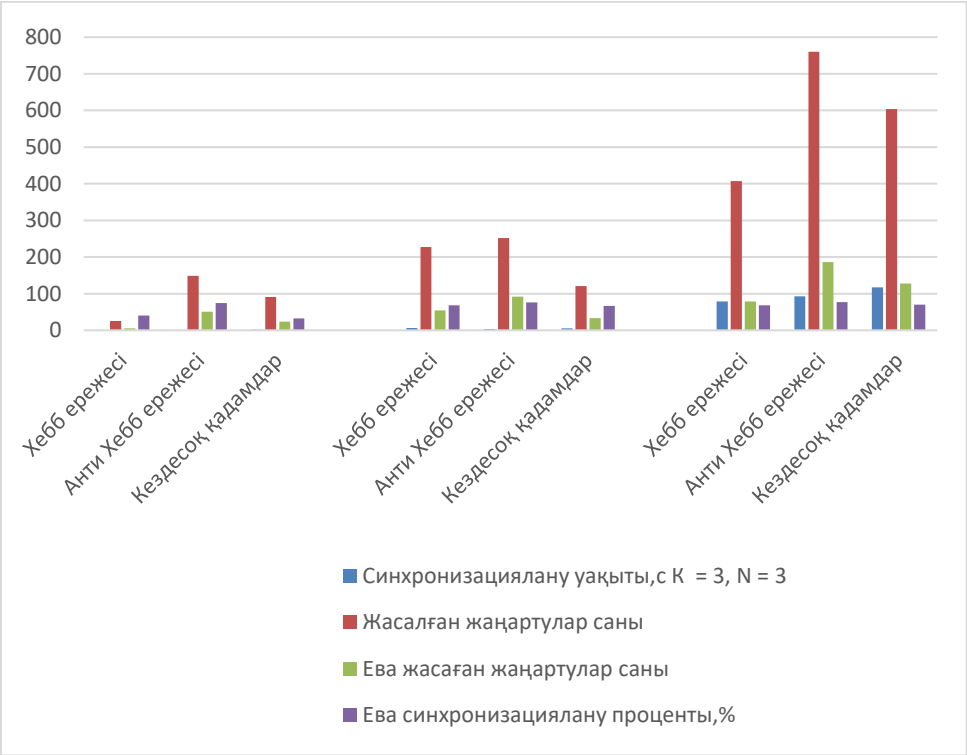
$$w_{k,n}{}' = g\left(w_{k,n} - \theta(\sigma_k, \tau)\theta(\tau_A, \tau_B)x_{k,n}\sigma\right) \quad (11)$$

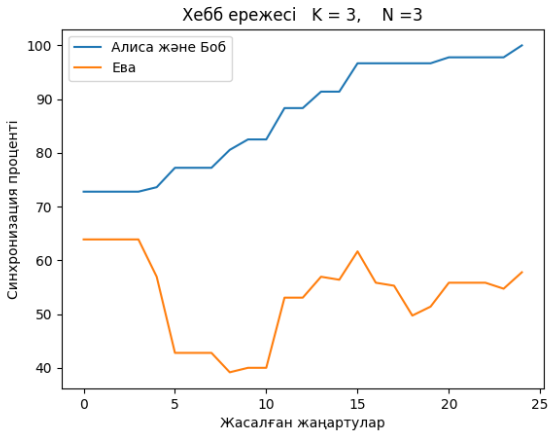
$$w_{k,n}{}' = g\left(w_{k,n} + \theta(\sigma_k, \tau)\theta(\tau_A, \tau_B)x_{k,n}\right) \quad (12)$$

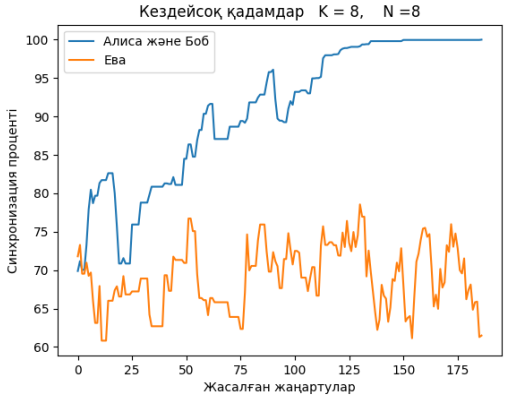
Қарастырылған нейрондық желі көмегімен кілт алмастыру әдісін қауіпсіздігі, оның жасырын қабатындағы перцептрон мәні тек желі иесінен басқа ешкімге белгілі еместігі көмегімен жүзеге асады. Үшінші жақтың (Ева деп алайық) нейрондық желісі Алиса мен Бобтың нейрондық желілерімен синхронизациялануы үшін жасырын қабаттағы нейрондар мәнін білу қажет. Себебі, оқыту кезінде салмақ мәндері жасырын қабаттағы мәндер көмегімен жаңарады (10,11,12 теңдеулер).

Кесте 1. Әртүрлі параметрлер кезінде оқыту ережелері көмегімен алынған нәтижелер

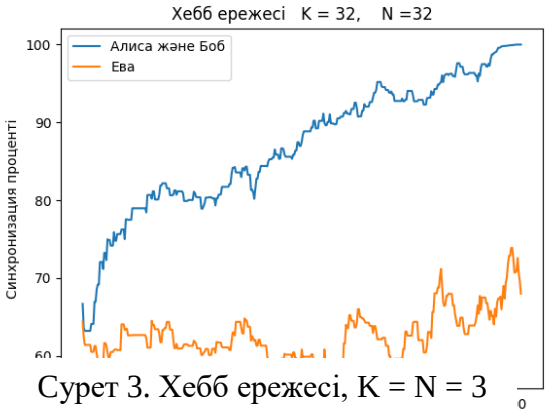
	Синхронизациялану уақыты,с	Жасалған жаңартулар саны	Ева жасаған жаңартулар саны	Ева синхронизациялану проценты,%
	К = 3, N = 3			
Хебб ережесі	0,077999115	25	5	40
Анти Хебб ережес	0,666000605	149	51	74
Кездесоқ қадамдар	1,98	91	24	32,61
	К = 8, N = 8			
Хебб ережесі	6,31	227	54	68,28
Анти Хебб ережес	3,27	252	92	75,78
Кездесоқ қадамдар	5,23	121	33	66,48
	К = 32, N = 32			
Хебб ережесі	78,93	407	79	67,97
Анти Хебб ережес	92,32	760	186	76,71
Кездесоқ қадамдар	116,92	604	128	69,65



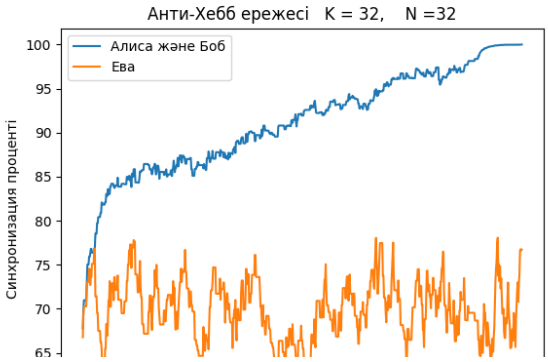




Сурет 2. Әртүрлі параметрлер кезінде оқыту ережелері көмегімен алынған нәтижелер



Сурет 3. Хебб ережесі, K = N = 3



Сурет 4. Кездейсоқ қадамдар, K=N=8

Сурет 5. Хебб ережесі, K = N = 32

Сурет 6. Анти - Хебб ережесі, K = N = 32

Қолданылған әдебиеттер тізімі

1. Klimov A., Mityagin A., Shamir A. Analysis of Neural Cryptography. ASIACRYPT ‘02 Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Berlin, Heidelberg: 2002. P. 288–298.

2. Sowmya D., Priyanka B.R. Design of Word Based Stream Cipher using Tree Parity Machine. Imperial Journal of Interdisciplinary Research. 2016. [Electronic resource]. URL: https://www.onlinejournal.in/IJIRV2I10/208.pdf.

3. Martın Abadi, David G. Andersen. Learning to protect communications with adversarial neural cryptography. 2016. [Electronic resource]. URL: https://arxiv.org/pdf/1610.06918.pdf

ӘОЖ 622.276

МҰНАЙ КЕН ОРНЫН ИГЕРУ ПРОЦЕСІНІҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕУІ ТУРАЛЫ

Әшімов Аңсар
a_ashim02@mail.ru
Л.Н.Гумилев атындағы ЕҰУ «6В06105- Математикалық және компьютерлік модельдеу» мамандығының 4 курс студенті, Астана, Қазақстан
Ғылыми жетекшісі- К.М. Сулейменов

Кіріспе

Мұнай кен орнының геологиялық құрылымы мен дамуын компьютерлік модельдеу жүйелері мұнай өндіруші компаниялардың геологиялық бөлімшелерінде жұмыс істейтін бағдарламалық қамтамасыз етудің маңызды бөлігі болып табылады[1,2]. Оларды пайдалану мұнай кен орындарын игеру, есеп құжаттамасын дайындау үрдісінде тактикалық және стратегиялық шешімдер қабылдауда қызметкерлердің тиімділігін айтарлықтай арттыруға мүмкіндік береді. Қазіргі уақытта геологиялық және гидродинамикалық модельдеу мәселелерін шешу үрдісін сол немесе басқа дәрежеде автоматтандыратын бағдарламалық құралдардың үлкен жиынтығы бар. Шартты түрде оларды екі үлкен топқа бөлуге болады: