УДК 004.4

Аспір. В.Л. Кімак[1] *– Івано-Франківський НТУ нафти і газу*

АРХІТЕКТУРА СПЕЦПРОЦЕСОРА ШИФРУВАННЯ ДАНИХ У ТЕОРЕТИКО-ЧИСЛОВОМУ БАЗИСІ РАДЕМАХЕРА-КРЕСТЕНСОНА

Результати аналізу стану захисту інформаційних потоків (ІП) у комп'ютеризованих системах свідчать, що загалом стан розв'язання цієї задачі далекий від досконалості. Тим більше, що виникає потреба у побудові стійких і продуктивних методів та алгоритмів шифрування ІП у комп'ютерних мережах з урахуванням тенденцій зростання вимог до необхідного рівня захисту різних типів ІП. Тому розроблення підходів, методів, алгоритмів, криптографічних комп'ютерних засобів захисту інформації з використанням мережевих технологій та високопродуктивних спецпроцесорів, особливо для проблемно-орієнтованих (ПОКС) та спеціалізованих комп'ютерних систем (СКС) на основі різних теоретико-числових базисів (ТЧБ) є актуальною науковою задачею. На основі алгоритмів та схемо-технічних рішень апаратних компонентів процесорів шифрування даних у теоретико-числовому базисі Радемахера-Крестенсона розроблено архітектуру багаторозрядного спецпроцесора шифрування даних, а також розраховано системи взаємопростих модулів для цих процесорів.

Ключові слова: алгоритм, спецпроцесор, шифрування даних, модульне експоненціювання, теоретико-числовий базис Радемахера-Крестенсона.

Вступ. Перспективним напрямком удосконалення алгоритмів криптозахисту даних на низових рівнях комп'ютерних систем є реалізація глибокого розпаралелення блоків даних на основі системи залишкових класів ТЧБ Крестенсона, при цьому виникає потреба вирішення задачі ефективного формування системи взаємопростих модулів багаторозрядних спецпроцесорів (1024 і більше біт) та оптимізованого синтезу їх компонентів у вигляді матрично-модульних утиліт, реалізованих на ПЛІС.

Модульне експоненціювання у ТЧБ Радемахера-Крестенсона. Теоретичною основою розмежованої системи числення залишкових класів (РСЗК) є цілочисельна форма системи залишкових класів (СЗК), рівняння якої представлено у вигляді суми **[**1**]**

$$N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk},$$

де N_{ik} – m-розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення. Тобто 1024-розрядний процесор СЗК (N_k) можна розмежувати на 32 фрагменти (n) по 32 біти (m) (рис. 1).

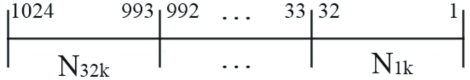

Рис. 1. Приклад розмежування 1024-розрядного процесора

Таким чином, пряме перетворення РСЗК набуває вигляду

$$N_k = \begin{cases} b_1 = (b_{11}+b_{21}+...+b_{r1}+...+b_{n1}) \bmod p_1 \\ b_2 = (b_{12}+b_{22}+...+b_{r2}+...+b_{n2}) \bmod p_2 \\ ... \\ b_i = (b_{1i}+b_{2i}+...+b_{ri}+...+b_{ni}) \bmod p_i \\ ... \\ b_k = (b_{1k}+b_{2k}+...+b_{rk}+...+b_{nk}) \bmod p_k \end{cases},$$

[1] Наук. керівник: проф. Я.М. Николайчук, д-р техн. наук – Тернопільський НЕУ

де: b_{ij} – залишок числа; i – порядковий номер модуля р; j – порядковий номер біта двійкового числа.

При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще більш глибокий рівень розпаралелення оброблення інформації, і, відповідно, підвищення швидкодії процесора СЗК **[**2, 3**]**.

Зі структури розмежованого процесора зрозуміло, що вона потребує обчислення залишків для кожного компонента згідно з виразом

$$b_{ij} = resN_{ij} (\bmod p_i),$$

де res – символ операції отримання залишку. Звідки, загальний залишок

$$b_i = res(b_{i1} + b_{i2} + ... + b_{in}) \bmod p_i.$$

За бітового розмежування двійкових чисел базису Радемахера, структура розмежування має вигляд, зображений на рис. 2.

Рис. 2. Бітове розмежування двійкового числа

Внаслідок такого розмежування двійкового числа (x_{n-1}, …, x_i, …, x_0) формується матриця залишків кожного і-го розряду у системі взаємопростих модулів p_1,…, p_j, …, p_k (табл. 1). Для переходу в базис Крестенсона над елементами рядків матриці, поданої в табл. 1, виконується така операція:

$$b_j = res(b_{n-1,j} + b_{n-2,j} + ... + b_{i,j} + ... + b_{1,j} + b_{0,j}) \bmod p_j.$$

Для виконання операції модульного експоненціювання запропонуємо використовувати матрицю, представлену у вигляді табл. 2, розмірність якої дорівнює розрядності n модуля р **[**1**]**. Причому в стовбцях табл. 2 подано значення $a^{2^i} \bmod p$ у базисі Радемахера $a_{i\,j}$ = 0,1. Для зменшення часової складності, степінь х записується степенями двійки і результат операції модульного експоненціювання отримується шляхом перемноження відповідної кількості стовпців з використанням методу модульного множення в розмежованій системі числення Радемахера-Крестенсона.

У запропонованому алгоритмі модульного експоненціювання, в якому на відміну від відомих, здійснюється заміна операції множення багаторозрядних чисел операцією сумування, що дає змогу зменшити обчислювальну складність та збільшити швидкодію.

Табл. 1. Матриця залишків числа x

	x_{n-1}	…	x_i	…	x_0
p_1	$b_{n-1,1}$	…	$b_{i,1}$	…	$b_{0,1}$
…	…	…	…	…	…
p_j	$b_{n-1,j}$	…	$b_{i,j}$	…	$b_{0,j}$
…	…	…	…	…	…
p_k	$b_{n-1,k}$	…	$b_{i,k}$	…	$b_{0,k}$

Табл. 2. Матриця піднесення до степеня в розмежованій системі числення Радемахера-Крестенсона

$a_{n-1\,n-1}$	…	$a_{i\,n-1}$	…	$a_{0\,n-1}$
…	…	…	…	…
$a_{n-1\,j}$	…	$a_{i\,j}$	…	$a_{0\,j}$
…	…	…	…	…
$a^{2^{n-1}}$	…	a^{2^i}	…	a^{2^0}

Розроблення структури спецпроцесора модульного експоненціювання. На основі матричного способу, а також апаратних реалізацій **[**4, 5**]** розроблено структуру спецпроцесора модульного експоненціювання багаторозрядних чисел у розмежованій системі числення Радемахера-Крестенсона (рис. 3).

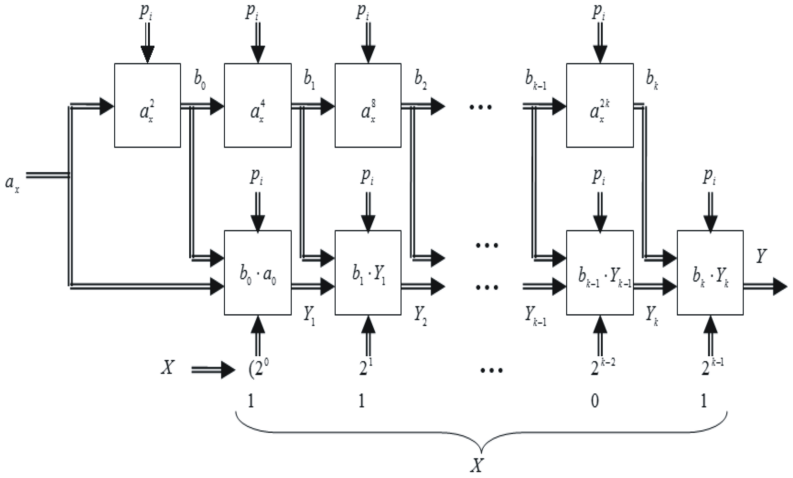

Рис. 3. Структура спецпроцесора модульного експоненціювання

Особливістю цієї структури є конвеєрне виконання операцій. Спочатку обчислюється $a_0^2 \bmod p$, після якого паралельно виконується обчислення квадрата по модулю поточного залишку b_i та добутку поточних залишків b_i і Y_i по модулю. Внаслідок такого конвеєра обчислення займає n+2 цикли обчислення квадратів по модулю. Структура компонента для обчислення квадратів та добутків по модулю (рис. 4) є однакова, але за обчислення квадратів подаються однакові коди $a_i = a_j$, а добутків – різні коди.

Таким чином, швидкодія цього спецпроцесора принципово залежить від швидкодії компонента, зображеного на рис. 4. Тому проблема підвищення швидкодії цього компонента, який може бути реалізований у різних теоретико-числових базисах, теоретично може бути виконана у 100-1000 разів швидше завдяки запропонованому вдосконаленню.

Компонентами цього спецпроцесора виступають також швидкодіючий двійковий суматор по модулю з парафазними наскрізними переносами (рис. 5) та швидкодіючий двійковий суматор (рис. 6).

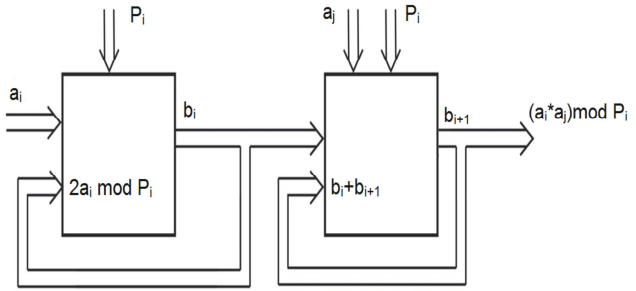

Рис. 4. Структура компонента для обчислення добутку багаторозрядних чисел по модулю

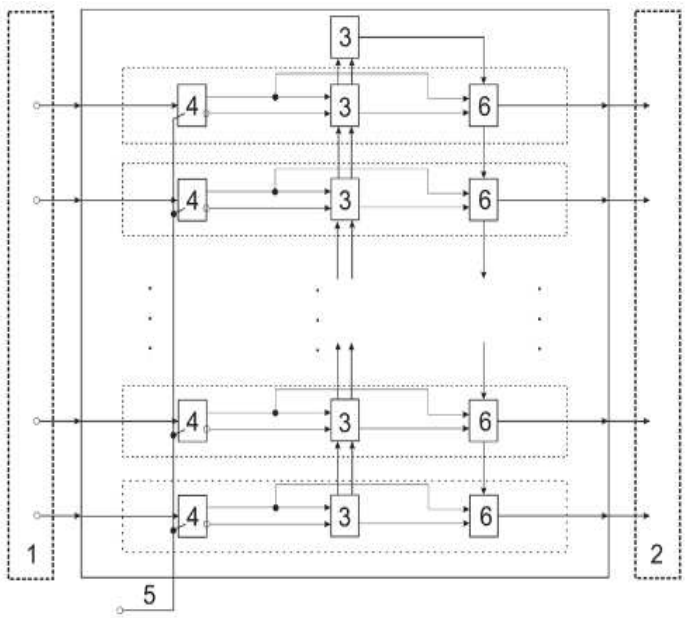

Рис. 5. Функціональна структура швидкодіючого двійкового суматора по модулю з парафазними наскрізними переносами

Швидкодіючий двійковий суматор по модулю з парафазними наскрізними переносами – патент України №90144 [6] (див. рис. 5). Після подачі сигналу синхронізації у вигляді фронту наростання на вхідну шину 5 вхідний код даних записується в тригер 4 відповідного розряду суматора 3. Вихідні коди тригерів подаються на відповідні входи нульових чи одиничних спеціалізованих однорозрядних суматорів відповідного доповнювального коду модуля $P_д$. Внаслідок сумування вхідного коду з кодом $P_д$ та всіх наскрізних переносів у суматорах пристрою на виході 2^k знакового розряду однорозрядного суматора (S_k) формується потенціал: 0, якщо $a \geq P$, тоді $b = (a+P_0) \bmod P$, інакше $a < P$ і b=a. Отриманий код b з виходів мультиплексорів 6 поступає на вихідну шину пристрою 2. Цей компонент використовується для виконання операції $(a+P_д)$

mod P, де $P_д$ – доповнювальний код числа P ($P_c = \vec{P} + 1$), який використовується в системах шифрування даних.

Ще одним компонентом спецпроцесора є **швидкодіючий двійковий суматор – патент України №97162 [7]** (див. рис. 6). Суматор працює таким чином: на вхідні шини 1 і 2 подаються коди операндів операції сумування, на вхід 6 подається сигнал логічної одиниці. По сигналу синхронізації 4 в D-тригери 7 записується двійковий код першого операнда, а D-тригери регістра зсуву встановлюються в стан "1" по S-входах. При цьому в елементах 8 виконуються паралельні операції сумування з наскрізними переносами, а на виходах елементів 9 формуються сигнали, які встановлюють D-тригери регістра зсуву по R-входах в нульовий стан. Під дією сигналу синхронізації шини 5, починаючи з тригерів, які знаходяться в стані "0", записуються нулі в групах розрядів, на які поширюються наскрізні переноси. Після завершення групи з найбільшим числом розрядів між тригерами, які знаходяться в нульових станах на виході ланцюга 11, формується сигнал пришвидшеного завершення сумування 12.

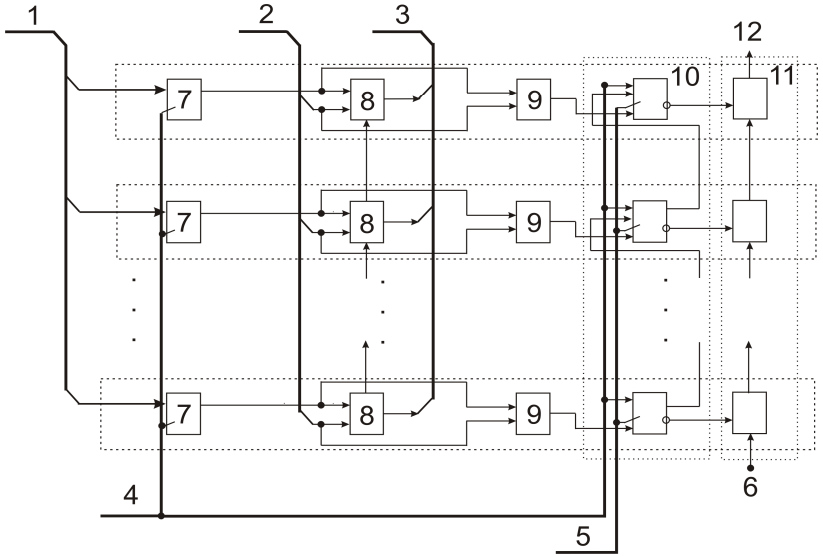

Рис. 6. Функціональна структура швидкодіючого двійкового суматора

При цьому розрядності процесора в базисі Радемахера 2^k потрібну розрядність спецпроцесора у базисі Крестенсона потрібно розраховувати згідно з виразом

$$N = \hat{E}\left[\log_2(P-1)\right] \geq 2^k + 2,$$

де $\hat{E}[\bullet]$ – цілочисельна функція з заокругленням до більшого цілого;

$$P = \prod_{i=1}^{n} p_i,$$

де: $p_i \in (p_1, p_2, ..., p_i, ..., p_n)$ – набір взаємопростих модулів з розрядністю $\hat{E}\left[\log_2(P-1)\right] \leq \frac{N}{n}$; $P \in \overline{0, N-1}$ – діапазон кодування чисел у базисі Крестенсона.

В основу методу вибору системи взаємопростих модулів для великорозрядних процесорів базису Крестенсона покладено такий алгоритм:

1) вибирається модуль $p_1 = 2^k$ з виконанням умови $\hat{E}\left[\log_2(2^k - 1)\right] = n$, оскільки $b_{i\_\max} = p_i - 1$;
2) вибираються всі прості числа розрядністю n в діапазоні $\hat{E}\left[\log_2(2^k - 1)\right] \div \hat{E}\left[\log_2(2^{k-1} + 1)\right]$, тобто 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,1009, 1013, 1019, 1021 при n=10;
3) вибираються добутки простих чисел, сумарна розрядність яких відповідає n-біт;
4) вибираються прості числа розрядність яких дорівнює (n-1)-біт.

Внаслідок використання розробленого алгоритму отримано набори модулів для процесорів з розрядністю 256, 512 та 1024 біти.

Висновки. Використання ТЧБ Радемахера-Крестенсона у задачах шифрування даних дає змогу ефективно застосувати матричні методи під час побудови спецпроцесорів шифрування, а заміна операцій множення операціями додавання на етапах генерації ключів, шифрування та дешифрування – значно зменшити часову складність залежно від розрядності параметрів алгоритмів шифрування. Розраховано системи взаємопростих модулів для багаторозрядних процесорів, які реалізують арифметично-логічні операції у базисі Крестенсона і дають змогу шифрувати багаторозрядні масиви даних у реальному часі, а також підвищують регулярність архітектури багаторозрядних процесорів.

Література

1. Николайчук Я.М. Коди поля Галуа: теорія та застосування : монографія / Я.М. Николайчук. – Тернопіль : Вид-во ТНЕУ. – 2012. – С. 239-249.

2. Николайчук Я.М. Теорія джерел інформації" : монографія / Я.М. Николайчук. – Тернопіль : Вид-во ТНЕУ, 2008. – 536 с.

3. Kasyanchuk M. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Basis / M. Kasyanchuk, I. Yakymenko, Ya. Nykolaychuk // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET–2010) : Proceedings of the Xth International Conference. – Lviv-Slavsk. – 2010. – C. 241.

4. Tsanko R. Theory, Topology and Building Technology of Multibasis Specialized Processor / R. Tsanko, O. Volynskyy, V. Puyul, I. Pituh // Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET-2012) : Proceedings of the XIth International conference. – Lviv-Slavsk. – 2012. – C. 260.

5. Круліковський Б.Б. Системні характеристики компонентів багаторозрядних процесорів шифрування даних / Б.Б. Круліковський, А.Я. Давлетова, В.Л. Кімак // Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ISCM-2014) : зб. матер. Міжнар. наукової координаційної наради. – Івано-Франківськ, 2014. – С. 105-107.

6. Патент на корисну модель № 90144 МПК G06F 7/00. Опублікований 12.05.2014 Бюл. № 9. Николайчук Я.М, Кімак В.Л., Волинський О.І., Круліковський Б.Б. / Пристрій визначення залишку по модулю багаторозрядного числа.

7. Патент на корисну модель № 97162 МПК G06F 7/00. Опублікований 10.03.2015 Бюл. № 5. Николайчук Я.М, Кімак В.Л., Круліковський Б.Б. / Пристрій додавання багаторозрядних двійкових чисел.

Кимак В.Л. **Архитектура спецпроцессора шифрования данных в теоретико-числовом базисе Радемахера-Крестенсона**

Результаты анализа состояния защиты информационных потоков (ИП) в компьютеризированных системах свидетельствует, что в целом состояние решения этой задачи далеко от совершенства. Тем более, что возникает потребность в построении устойчивых и продуктивных методов и алгоритмов шифрования ИП в компьютерных сетях с учетом тенденций роста требований к необходимому уровню защиты различных типов ИП. Поэтому разработка подходов, методов, алгоритмов, криптографических компьютерных средств защиты информации с использованием сетевых технологий и высокопроизводительных спецпроцессоров, особенно для проблемно-ориентированных (ПОКС) и специализированных компьютерных систем (СКС) на основе различных теоретико-числовых базисов (ТЧБ) является актуальной научной задачей. На основе алгоритмов и схемотехнических решений аппаратных компонентов процессоров шифрования данных в теоретико-числовом базисе Радемахера-Крестенсона разработана архитектура многоразрядного спецпроцессора шифрования данных, а также рассчитаны системы взаимнопростых модулей для этих процессоров.

Ключевые слова: алгоритм, спецпроцессор, шифрование данных, модульное экспоненцианирование, теоретико-числовой базис Радемахера-Крестенсона.

Kimak V.L. **The Architecture of Special Processor for Data Encryption in Rademacher-Krestenson's Theoretical-Numerical Basis**

The analysis of information flow protection (IF) in the computer systems indicates that the overall condition of solving this problem is far from perfect. Moreover, there is a need to build stable and productive methods of IF encryption algorithms in computer networks with taking into account bigger requirements for data protection of various IF types. Therefore, the development of approaches, methods, algorithms, cryptographic computer information security using networking and high-performance special processors, especially for problem-oriented (POCS) and specialized computer systems (SCS) based on various theoretical and numerical bases (TNB) is an actual scientific task. Based on algorithms and schemes and technical solutions of processor's hardware components for data encryption in Rademacher-Krestenson's theoretical-numerical basis is developed special multibit processor architecture for data encryption and is calculated system of coprime modules designed for these processors.

Keywords: algorithm, special processors, data encryption, modular exponentiation, Rademacher-Krestenson's theoretical-numerical basis.

УДК 681.5:519.7

Доц. В.М. Коцовський, канд. техн. наук – Ужгородський НУ

КІЛЬКІСНІ ОЦІНКИ РОЗПІЗНАВАЛЬНОЇ ЗДАТНОСТІ ДВОПОРОГОВИХ НЕЙРОННИХ ЕЛЕМЕНТІВ

Досліджено властивості двопорогових нейронних елементів, які є одним з найпростіших узагальнень класичних нейроелементів МакКаллока-Піттса. Використання двопорогових нейронів дає змогу подолати деякі обмеження, притаманні звичайним пороговим елементам, зокрема знайти розв'язок відомої XOR-проблеми. Вивчено питання, які стосуються оцінки кількості дихотомій скінченної множини у n-вимірному просторі, які можна отримати за допомогою двопорогових нейронів. Також досліджено асимптотичну поведінку кількості дихотомій та розглянуто питання знаходження розмірності Вапніка-Червоненкіса двопорогових нейроелементів.

Ключові слова: нейронний елемент, двопороговий нейрон, штучна нейромережа, розпізнавання.

Вступ. Конекціоністський підхід ґрунтується на використанні нейромереж до моделювання складних об'єктів та явищ. Кілька останніх десятиріч штучні нейромережі та інші нейроподібні структури широко використовують для розв'язування широкого кола актуальних господарських задач **[**1**]**. Однією з ключових проблем, які постають у практичному застосуванні штучних нейронних мереж, є проблема вибору моделі нейронів, які утворюють нейромережу. Традиційними вважають підходи з використання нейронів з лінійним вхідним оператором та функцію активації порогового типу (пороговий елемент) або сигмоїдального типу (неперервний нейрон). Кожний з цих підходів має свої переваги і недоліки **[**2**]**.

Уведення до розгляду двопорогових нейронних елементів (ДНЕ) та їх дослідження мотивується у літературі більш потужними можливостями цих елементів порівняно із звичайними пороговими елементами з розпізнавання належності точок у R^n до одного з двох заданих класів. Це саме твердження стосується і нейронів із неперервними функціями активації двопорогового типу, до яких належить широкий клас "дзвіноподібних" функцій.

У роботах **[**3, 4**]** зроблено спробу кількісно оцінити переваги використання двопорогових нейроелементів. Зокрема, встановлено оцінки кількості класифікацій точок скінченної множини у дійсному векторному просторі, які можна отримати за допомогою ДНЕ. Варто зауважити, що в асимптотичному сенсі встановлені оцінки мають різний порядок росту. У пропонованій роботі з використанням прийомів теорії лінійних нерівностей вдалося отримати та обґрунтувати уточнені оцінки кількості різних двопорогових класифікацій.

Модель двопорогового нейрона. Нехай R^n – n-вимірний дійсний евклідів простір. Якщо $\mathbf{w}=(w_1,w_2,\ldots,w_n)\in \mathrm{R}^n$, $\mathbf{x}\in(x_1,x_2,\ldots,x_n)\in \mathrm{R}^n$, то величину скалярного добутку

$$(\mathbf{w},\mathbf{x})=\sum_{i=1}^{n} w_i x_i$$

будемо називати зваженою сумою, що відповідає вектору **x**.

Штучним двопороговим дійсним нейронним елементом з ваговим вектором $\mathbf{w}\in \mathrm{R}^n$, порогами $t_1,t_2\in \mathrm{R}$ $(t_1<t_2)$ будемо називати функціональний елемент з n дійсними входами $x_1,x_2,\ldots,x_n$ та одним виходом $y\in\{-1,1\}$, поведінка якого описується співвідношеннями:

$$y=\begin{cases}-1, & t_1<(\mathbf{w},\mathbf{x})<t_2,\\ 1, & (\mathbf{w},\mathbf{x})\le t_1\vee(\mathbf{w},\mathbf{x})\ge t_2.\end{cases}$$

У термінах **[**2**]** зважена сума є вхідним оператором ДНЕ із функцією активації вигляду

$$f_{t_1,t_2}(x)=\begin{cases}-1, & t_1<x<t_2,\\ 1, & x<t_1\vee x>t_2.\end{cases}$$

ДНЕ повністю визначається впорядкованою трійкою $(\mathbf{w},t_1,t_2)$, яку будемо надалі називати вектором структури або просто структурою ДНЕ.