Issue 9, 2021

https://doi.org/10.23939/sisn2021.09.084

УДК 004.8.032.26

РОЗРОБЛЕННЯ МОБІЛЬНИХ ЗАСОБІВ НЕЙРОПОДІБНОГО КРИПТОГРАФІЧНОГО ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

Іван Цмоць[1], Василь Рабик[2], Юрій Лукащук[3]

[1, 3] Національний університет "Львівська політехніка"
[2] Львівський національний університет імені Івана Франка
[1] ivan.tsmots@gmail.com, ORCID 0000-0002-4033-8618
[2] vasyl.rabyk@lnu.edu.ua, ORCID 0000-0003-2655-0812
[3] urijlukas@gmail.com, ORCID 0000-0002-8933-8635

Сформовано вимоги, вибрано метод і розглянуто основні етапи розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі. Показано, що розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі з високою ефективністю використання обладнання зводиться до мінімізації апаратних затрат із забезпеченням множини вимог, характеристик і обмежень. Вдосконалено таблично-алгоритмічний метод обчислення скалярного добутку завдяки можливості роботи з операндами з плаваючою комою та орієнтовано його на апаратно-програмну реалізацію. Розроблено на базі універсального процесорного ядра, доповненого спеціалізованими модулями, мобільні засоби нейроподібного криптографічного шифрування та дешифрування даних, які за рахунок взаємопоєднання універсального та спеціалізованого підходів, програмних і апаратних засобів забезпечують ефективну реалізацію алгоритмів криптографічного шифрування та дешифрування даних у реальному часі. Запропоновано для досягнення високих техніко-економічних показників під час реалізації спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі використовувати багатооперандний підхід, таблиці макрочасткових добутків і базис елементарних арифметичних операцій. Реалізовано з використанням мови програмування апаратури VHDL та середовища розроблення Quartus II вер. 13.1 на FPGA спеціалізовані модулі нейроподібного криптографічного шифрування та дешифрування даних. Здійснено оцінювання апаратних і часових параметрів розробленого спеціалізованого модуля нейроподібного криптографічного дешифрування даних.

Ключові слова: шифрування даних; дешифрування даних; нейронна мережа; скалярний добуток; спеціалізований модуль; нейроподібний елемент; FPGA.

Постановка проблеми

У військовій галузі, де широко використовуються мобільні інтелектуальні роботи, безпілотні літальні апарати, мікросупутники, різноманітні мобільні транспортні системи, автоматизовані системи управління озброєнням, важливою проблемою є забезпечення криптографічного захисту зв'язку між цими засобами та стаціонарним центром керування. Для вирішення такої проблеми розробляють мобільні засоби криптографічного шифрування та дешифрування даних у реальному часі, які є основою бортових систем криптографічного захисту та передавання даних (СКЗПД). Під час розроблення мобільних засобів криптографічного захисту бортових СКЗПД виникає проблема забезпечення режиму

реального часу, підвищення криптостійкості, завадостійкості та зменшення маси, габаритів, енергоспоживання та вартості. Одним зі способів забезпечення високих техніко-економічних характеристик мобільних засобів криптографічного захисту бортових СКЗПД є використання для криптографічного захисту автоасоціативної нейроподібної мережі прямого поширення, яка навчається на основі методу головних компонент. Особливістю таких нейроподібних мережах є можливість наперед обчислити вагові коефіцієнти, що дасть змогу використати таблично-алгоритмічний метод для реалізації нейроподібних елементів. Розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних з високими техніко-економічними показниками потребує широкого використання сучасних технологій надвеликих інтегральних схем (НВІС), розроблення нових методів, алгоритмів і НВІС-структур, орієнтованих на ефективну реалізацію алгоритмів нейромережевого криптологічного шифрування та дешифрування даних.

Одним зі способів реалізації мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних є використання універсального процесорного ядра, доповненого спеціалізованими апаратно-програмними засобами. Завдяки взаємопроникненню універсального та спеціалізованого, програмного й апаратного забезпечення уможливлюється ефективна реалізація алгоритмів нейромережевого криптографічного шифрування та дешифрування даних. Використання під час розроблення мобільних засобів нейромережевого криптографічного шифрування та дешифрування даних сучасної елементної бази (мікроконтролерів, ПЛІС типу FPGA) забезпечує обмеження щодо маси, габаритів і енерогоспоживання. Реалізація спеціалізованих апаратних засобів криптографічного шифрування та дешифрування даних на FPGA забезпечує можливість зміни структури та нарощування функцій. Нейроподібне криптографічне шифрування та дешифрування даних у реальному часі досягається за рахунок використання розпаралелення процесів шифрування та дешифрування даних і апаратної реалізації нейроподібних елементів на основі багатооперандного підходу, таблиць макрочасткових добутків і базису елементарних арифметичних операцій.

Тому актуальною проблемою є реалізація мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі з високими техніко-економічними показниками.

Аналіз останніх досліджень та публікацій

Аналіз основних тенденцій розвитку бортових систем криптографічного захисту даних у реальному часі показує, що для виконання шифрування та дешифрування даних у таких системах все більше використовують нейромережеві методи [1–5]. Аналіз засобів криптографічного захисту даних, які використовують нейромережеві методи, показує, що їх реалізація переважно виконується програмно. Основним недоліком програмної реалізації нейромережевого криптографічного захисту даних є складність забезпечення режиму реального часу та обмежень щодо маси, габаритів, енергоспоживання та вартості СКЗПД.

У роботах [1–5] здійснено адаптацію автоасоціативної нейронної мережі з неітераційним навчанням для задач криптографічного шифрування та дешифрування даних. У такій нейромережі вагові коефіцієнти обчислюються у результаті її навчання на основі методу головних компонент. Особливістю цього методу є використання системи власних векторів, які відповідають власним значенням коваріаційної матриці вхідних даних [6–8]. Автоасоціативна нейромережа з обчисленими ваговими коефіцієнти є нейроподібною мережею, яка орієнтована на криптографічний захист даних. У роботі [8] показано, що ключем нейроподібного криптографічного захисту даних є коди маскування, архітектура нейроподібної мережі та матриця вагових коефіцієнтів.

Аналіз нейроподібних засобів [9–11], які використовують для криптографічного шифрування та дешифрування даних, показав, що основа таких засобів – нейроподібні елементи. Особливістю таких нейроелементів є те, що їх реалізація зводиться до обчислення скалярного добутку з використанням попередньо визначених вагових коефіцієнтів.

Аналіз методів обчислення скалярного добутку з ваговими коефіцієнтами, які є наперед відомими [12–15], показав, що одним із найефективнішних методів є таблично-алгоритмічний, який зводиться до операцій читання макрочасткових добутків, додавання та зсуву. Недоліком цього методу є

те, що він орієнтований на роботу із вхідними даними та ваговими коефіцієнтами у форматі із фіксованою комою.

Мета та завдання дослідження

Мета роботи – розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних у реальному часі з високими техніко-економічними характеристиками. Досягнення поставленої у роботі мети передбачає виконання таких завдань:

- визначення вимог та вибір методу розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних;
- удосконалення таблично-алгоритмічного методу обчислення скалярного добутку;
- розроблення структури мобільних засобів нейроподібного криптографічного шифрування даних;
- розроблення структури мобільних засобів нейроподібного криптографічного дешифрування даних;
- реалізація спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних на FPGA.

Основні результати дослідження

1. Визначення вимог та вибір методу розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних

Розроблення мобільних засобів нейромережевого криптографічного шифрування та дешифрування даних вимагає широкого використання сучасної елементної бази, розроблення нових методів, алгоритмів і структур, орієнтованих на ефективну апаратно-програмну реалізацію нейроподібних алгоритмів шифрування та дешифрування даних. Під час розроблення таких мобільних засобів виникає проблема забезпечення режиму реального часу, підвищення криптостійкості із одночасним зменшенням маси, габаритів, енергоспоживання та вартості. Для забезпечення реального часу процеси нейроподібного шифрування та дешифрування даних повинні відбуватися без накопичення затримок, а час шифрування $t_ш$ та час дешифрування $t_д$ повинні бути однаковими. Виконання шифрування даних у реальному часі накладає обмеження на час $t_ш$, який не повинен перевищувати часу надходження даних $t_{нд}$, тобто:

$$t_ш \le t_{нд} . \tag{1}$$

Час надходження даних $t_{нд}$ залежить як від обсягу N, розрядності n і частоти F_d надходження вхідних даних X_j, де $j = 1,\ldots, N$, так і від кількості k каналів та їх розрядності n_k. Такий час визначають за формулою:

$$t_{нд} = \frac{Nn}{F_d k n_k} . \tag{2}$$

Для шифрування (дешифрування) потоків даних у реальному часі за допомогою апаратно-програмних засобів їх продуктивність повинна становити:

$$П = \frac{\beta R F_d k n_k}{Nn} , \tag{3}$$

де R – складність алгоритмів шифрування (дешифрування); β – коефіцієнт урахування особливостей засобів реалізації. Застосування мобільних засобів шифрування та дешифрування даних у галузях, де апаратура є бортовою, тобто такою, яку возять, носять, яка літає і плаває, накладає жорсткі обмеження на їхні масогабаритні характеристики. Одночасно до мобільних засобів шифрування та дешифрування даних ставлять жорсткі вимоги щодо споживаної потужності, яка впливає на габарити джерел живлення та засобів відведення тепла. Крім того, до мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних ставлять високі вимоги щодо живучості, надійності, а також забезпечення перевірки працездатності, швидкої локалізації та знешкодження несправностей. Щоб забезпечити достатньо високу живучість мобільних засобів шифрування та дешифрування даних, необхідна взаємозаміна структурних частин. Вирішити це завдання можна

тільки за умови однотипності складових частин засобів шифрування та дешифрування даних і однорідності їх архітектури.

Зменшення масогабаритних характеристик, енергоспоживання, підвищення надійності мобільних засобів СЗПД та забезпечення режиму реального часу можна досягти використанням сучасної елементної бази.

Завдання синтезу мобільних засобів криптографічного шифрування та дешифрування даних зводиться до формування множин вимог $\mathbf{R} = \{R_1, R_2,\ldots,R_k\}$, характеристик $\mathbf{H} = \{H_1, H_2,\ldots,H_m\}$, обмежень $\mathbf{B} = \{B_1, B_2,\ldots,B_k\}$ і знаходження такого вектора $\mathbf{H}^* = [H^*_1, H^*_2,\ldots,H^*_m]$, $H^*_i = f_i(R, H, B)$, $i = 1,\ldots, m$, який забезпечить максимальне значення ефективності використання обладнання $E = \max f(\mathrm{R}, \mathrm{H}^*,\mathrm{B})$.

Множина вимог **R** до модулів нейроподібного криптографічного шифрування та дешифрування даних складається із: R_1 – кількість нейроподібних елементів N; R_2 – розрядність входів m; R_3 – частота надходження повідомлень F_d; R_4 – швидкодія елементної бази, яка визначається часом затримки вентиля $t_в$; R_5 – розрядність повідомлення n; R_6 – матриця вагових коефіцієнтів W_{ji} R_7 – час життя ключа $t_{жк}$. Множину характеристик **H** становлять: H_1 – обсяг пам'яті ключів Q_1; H_2 – обсяг пам'яті кодів Q_2; H_3 – обсяг пам'яті макрочасткових добутків Q_3; H_4 – час шифрування даних $t_ш$; H_5 – час дешифрування даних $t_{дш}$; H_6 – час кодування даних $t_к$; H_7 – час декодування даних $t_{дк}$; H_8 – витрати обладнання на реалізацію нейроподібних елементів $W_{НЕ}$; H_9 – витрати обладнання на реалізацію блока кодування $W_{БК}$; H_{10} – витрати обладнання на реалізацію блока декодування $W_{БДк}$.

Обмеження **B**, які необхідно враховувати під час синтезу СЗПД у реальному часі з використанням шумоподібних кодів, є такими: B_1 – продуктивність програмно-апаратних засобів $П$; B_2 – швидкість передавання даних v; B_4 – потужність енергоспоживання P; B_5 – габарити S; B_6 – максимальна температура роботи t_{max}; B_7 – мінімальна температура роботи t_{min}; B_7 – маса M; B_8 – стійкість апаратних засобів до спецфакторів γ; B_8 – вартість апаратних засобів C_A; B_9 – вартість програмних засобів $C_П$; B_{10} – витрати на експлуатацію $C_{Екс}$

Здійснюючи синтез мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних, необхідно забезпечити вимоги технічного завдання та високу ефективність використання обладнання, що зв'язує продуктивність із витратами обладнання та дає оцінку елементам (вентилям) системи за продуктивністю. Кількісно ефективність використання обладнання визначається так:

$$E_{Мш/д} = \frac{\beta_з R}{W_{Мш/д} t_{ш/д}}, \tag{4}$$

де $\beta_з$ – коефіцієнт, який враховує особливості засобів реалізації алгоритмів шифрування та дешифрування; $W_{Мш/д}$ – апаратні затрати на реалізацію модулів шифрування та дешифрування даних; R – складність алгоритмів шифрування та дешифрування даних; $t_{ш/д}$ – час шифрування та дешифрування даних.

Вихідною інформацією для розроблення мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних є:

- методи реалізації алгоритмів (послідовні, паралельні) нейроподібного елемента;
- графове відображення алгоритмів реалізації;
- структури (рекурсивна, нерекурсивна) для реалізації нейроподібного елемента;
- кількість вхідних даних N та формат їх подання – із фіксованою або плаваючою комою;
- використання вагових коефіцієнтів у форматі із плаваючою комою;
- кількість нейронів і точність обчислень;
- інтенсивність надходження вхідних даних;
- вимоги до інтерфейсу;
- техніко-економічні вимоги й обмеження.

Загалом задачі синтезу мобільних засобів нейроподібного криптографічного шифрування та дешифрування даних можна сформулювати так:

- вибрати алгоритм нейроподібного шифрування та дешифрування даних та подати його у вигляді конкретизованого потокового графу;
- розробити структуру блоків нейроподібного шифрування та дешифрування даних із максимальною ефективністю використання обладнання, яка враховує всі обмеження та забезпечує оброблення даних у реальному масштабі часу;
- визначити основні характеристики нейроподібних елементів та здійснити їх синтез;
- вибрати способи обміну, визначити необхідні зв'язки та розробити систему обміну між компонентами блоків нейроподібного шифрування та дешифрування даних;
- визначити послідовність реалізації у часі алгоритму нейроподібного шифрування та дешифрування даних та розробити алгоритми управління процесом шифрування та дешифрування даних.

Синтез модулів нейроподібного криптографічного шифрування та дешифрування даних зводиться до виконання таких етапів:

1) вибір та розроблення алгоритму реалізації нейроподібного елемента;
2) розроблення структури нейроподібного елемента;
3) розроблення на основі нейроподібного елемента алгоритмів шифрування та дешифрування даних;
4) розроблення структури модулів нейроподібного криптографічного шифрування та дешифрування даних;
5) розроблення інтерфейсу зв'язку модулів нейроподібного криптографічного шифрування та дешифрування даних з навколишнім середовищем;
6) розроблення алгоритмів управління процесами шифрування та дешифрування даних;
7) обчислення синаптичних вагових коефіцієнтів;
8) обчислення таблиць макрочасткових добутків;
9) розроблення засобів верифікації роботи модулів нейроподібного криптографічного шифрування та дешифрування даних.

2. Удосконалення таблично-алгоритмічного методу обчислення скалярного добутку

Нейроподібні елементи, які використовують для криптографічного шифрування та дешифрування даних, ґрунтуються на операції обчислення скалярного добутку:

$$Z = \sum_{j=1}^{N} W_j X_j \,, \tag{5}$$

де N – кількість добутків; X_j – j-ті вхідні дані; W_j – j-й ваговий коефіцієнт.

Особливістю операції обчислення скалярного добутку, що використовується у нейроподібних елементах, є те, що вагові коефіцієнти W_j синаптичних зв'язків є попередньо обчисленими (константами) і їх задають у форматі з плаваючою комою $W_j = w_j 2^{p_{Wj}}$ (де w_j – мантиса W_j вагового коефіцієнта; p_{W_j} – порядок W_j вагового коефіцієнта). Вхідні дані, які надходять у форматі з плаваючою комою $X_j = x_j 2^{p_x}$ (де x_j – мантиса відповідно j-х вхідних даних X_j; p_x – порядок вхідних даних) для виконання операції обчислення скалярного добутку необхідно звести до найбільшого спільного порядку p_{xmaxc}. Для цього виконують такі операції: визначення найбільшого спільного порядку p_{xmaxc}; обчислення різниці порядків $\Delta p_{x_j} = p_{xmaxc} - p_{x_j}$; зсунення вправо на різницю порядків Δp_{x_j} мантиси x_j й отримання масштабованої мантиси x_j^h.

Для реалізації операцій обчислення скалярного добутку із наперед обчисленими ваговими коефіцієнтами W_j (константами) доцільно використовувати таблично-алгоритмічний метод обчислення. Такий метод ґрунтується на багатооперандному підході, за якого обчислення

скалярного добутку розглядається як виконання єдиної операції із використанням базису елементарних арифметичних операцій.

Базовою операцією таблично-алгоритмічного методу обчислення скалярного добутку є зчитування із таблиці мантиси i-го макрочасткового добутку r_{Mi} ($i = 1,\ldots, n$, де n – розрядність вхідних даних X_j) та її додавання до раніше накопичених сум мантис. Адреса зчитування з таблиці утворюється із i-х розрядів приведених мантис вхідних даних x_j. Базова операція виконується за формулою:

$$z_i = 2^{-1} z_{i-1} + r_{Mi}\,. \tag{6}$$

де $z_0 = 0$.

Табличне формування i-ї мантиси макрочасткового добутку r_{Mi} передбачає виконання таких дій:

1) приведення вагових коефіцієнтів W_j синаптичних зв'язків до найбільшого спільного порядку p_{Wmaxc} із виконанням таких операцій: визначення найбільшого спільного порядку вагових коефіцієнтів p_{Wmaxc}; обчислення різниці порядків для W_j вагового коефіцієнта $\Delta p_{W_j} = p_{Wmaxc} - p_{W_j}$; зміщення вправо мантиси w_j на різницю порядків Δp_{W_j} й отримання масштабованої мантиси w_j^h;

2) обчислення мантиси макрочасткового добутку за формулою:

$$r_{Mi} = \begin{cases} 0, \quad якщо \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 0 \\ w_1^h, \quad якщо \quad x_{1i} = 1, \quad x_{2i} = x_{3i} = \ldots = x_{Ni} = 0 \\ w_2^h, \quad якщо \quad x_{1i} = 0, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0 \\ w_1^h + w_2^h, \quad якщо \quad x_{1i} = 1, x_{2i} = 1, x_{3i} = \ldots = x_{Ni} = 0 \\ \vdots \\ w_2^h + \ldots + w_N^h, \cdots якщо \quad x_{1i} = 0, x_{2i} = x_{3i} = \ldots = x_{Ni} = 1 \\ w_1^h + w_2^h + \ldots + w_N^h, \quad якщо \quad x_{1i} = x_{2i} = x_{3i} = \ldots = x_{Ni} = 1 \end{cases}; \tag{7}$$

3) визначення кількості розрядів переповнення v_k ($k = 1, \ldots, 2^N$) для кожного можливого варіанта макрочасткового добутку p_{Mk}, який обчислюють за формулою (7);

4) визначення максимального значення $v_{\max}$, отримуваного для випадку, коли всі i-ті вхідні дані однакові $x_{ji} = 1$;

5) обчислення значення відкоригованого порядку $p_{r_{Mв}}$ макрочасткового добутку додаванням значення v_{max} до p_{Wmaxc};

6) вирівнювання значень усіх мантис макрочасткових добутків зміщенням їх вправо на $v_{\max}$ розрядів;

7) запис вирівняних значень мантис макрочасткових добутків у таблицю.

Порядок скалярного добутку p_z є сумою максимального спільного порядку p_{xmaxc} вхідних даних та відкоригованого порядку $p_{r_{Mв}}$ макрочасткового добутку, який обчислюють так

$$p_z = p_{x_{maxc}} + p_{r_{Mв}}\,.$$

Кількість можливих варіантів макрочасткових добутків r_{Mi} і відповідно обсяг таблиці визначають за формулою:

$$Q = 2^N\,. \tag{8}$$

Обсяг пам'яті можна зменшити, поділивши усі добутки N на частини N_1 та N_2. Для кожної із цих частин формують окремі таблиці макрочасткових добутків r_{N1Mi} та r_{N2Mi}. Таблиці для r_{N1Mi} та r_{N2Mi} можуть зберігатися в окремих блоках пам'яті або в одному блоці пам'яті. У разі використання двох блоків пам'яті

частини макрочасткових добутків r_{N1Mi} та r_{N2Mi} зчитуються за один такт, а у випадку одного – за два такти. Макрочастковий добуток r_{Mi} є сумою двох частин макрочасткових добутків r_{N1Mi} та r_{N2Mi}.

Удосконалення таблично-алгоритмічного методу обчислення скалярного добутку полягає у тому, що тепер він орієнтований на роботу із вхідними даними з плаваючою комою.

3. Розроблення структури мобільних засобів нейроподібного криптографічного шифрування даних

Мобільні засоби нейроподібного криптографічного шифрування даних реалізуються на основі універсального ядра, доповненого спеціалізованими модулями. Структура спеціалізованих модулів нейроподібного криптографічного шифрування даних визначається кількістю нейроподібних елементів, яку обчислюють за формулою:

$$N = \frac{m}{n}, \tag{9}$$

де m – розрядність повідомлення; n – розрядність входів. Архітектура нейроподібної мережі, яка є частиною ключа, визначається розрядністю повідомлення m та розрядністю входів n нейроподібного елемента. Наприклад, для m = 24 розряди кількість нейроподібних елементів N може становити 24, 12, 8, 6, 4, 3 і 2 із розрядністю входів n відповідно 1, 2, 3, 4, 6, 8 і 12.

Для ефективної роботи модуль криптографічного шифрування даних повинен забезпечувати: налаштування архітектури нейроподібної мережі, можливість змінювати маски, обчислювати матриці вагових коефіцієнтів W_j і таблиці макрочасткових добутків P_{Mi}. Структуру мобільних засобів нейроподібного криптографічного шифрування даних, яка відповідає таким вимогам, наведено на рис. 1.

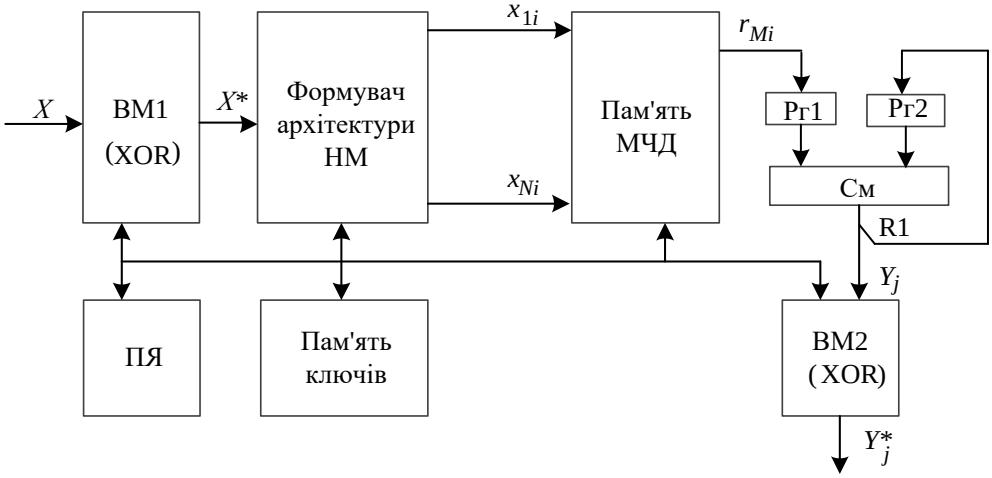

Рис. 1. Структура мобільних засобів нейроподібного криптографічного шифрування даних: ПЯ – процесорне ядро; ПК – пам'ять ключів; ВМ – вузол маски; НМ – нейроподібна мережа; МЧД – макрочасткові добутки; Рг – регістр; См – суматор

Перед початком шифрування даних ПЯ здійснюється налаштування архітектури нейроподібної мережі (кількості N та розрядності n входів). Для вибраної архітектури нейроподібної мережі за допомогою ПЯ обчислюють матрицю вагових коефіцієнтів W_j і таблиці макрочасткових добутків P_{Mi}, які записуються у пам'ять МЧД. Крім того, у вузли ВМ1 і ВМ2 записуються вибрані із пам'яті ключів маски. Повідомлення X, які необхідно зашифрувати, надходять на вхід ВМ1 у форматі з фіксованою комою. Повідомлення з накладеною маскою X* з виходу ВМ1 надходять на вхід нейроподібної мережі, де їх розділяють на N входів розрядністю n. На виході нейроподібної мережі формується адреса A_i для зчитування із пам'яті МЧД макрочасткового добутку r_{Mi}, який записується у регістр Рг1. За допомогою суматора См виконується підсумовування макрочасткових добутків r_{Mi} за формулою (6). Обчислений скалярний добуток передається у вузол ВМ2, де на нього накладається маска.

Особливістю спеціалізованих засобів нейроподібного криптографічного шифрування даних є одна пам'ять МЧД, у яку записуються макрочасткові добутки для N нейроподібних елементів і один

суматор См. Обчислення *N* скалярних добутків відбувається послідовно у часі. Кількість тактів, потрібних для обчислення одного скалярного добутку, визначається розрядністю входів *n*. Для обчислення *N* скалярних добутків на одному суматорі См необхідно виконати *m* тактів читання та додавання макрочасткових добутків. Управляє процесом шифрування у модулі ПЯ.

4. Розроблення структури мобільних засобів нейроподібного криптографічного дешифрування даних

Структура мобільних засобів нейроподібного криптографічного дешифрування даних визначається параметрами ключа, основними із яких є кількість нейроподібних елементів. Можливі варіанти ключів та їх параметри (маски, кількість нейроподібних елементів, матриця вагових коефіцієнтів) зберігаються у пам'яті ПК. Крім того, на вибір структури спеціалізованих засобів нейроподібного криптографічного дешифрування даних впливає те, що зашифровані дані Y_j надходять у форматі з плаваючою комою, а мантиса дорівнює 24 розрядам. Розрядність мантиси визначає кількість тактів, які необхідні для обчислення скалярного добутку. Тому для зменшення часу дешифрування даних запропоновано обчислення *N* скалярних добутків виконувати паралельно. Паралельне обчислення *N* скалярних добутків потребує використання для нейроподібного дешифрування даних *N* трактів обчислення скалярних добутків. Структуру мобільних засобів нейроподібного криптографічного дешифрування даних із використанням *N* трактів обчислення скалярних добутків наведено на рис. 2.

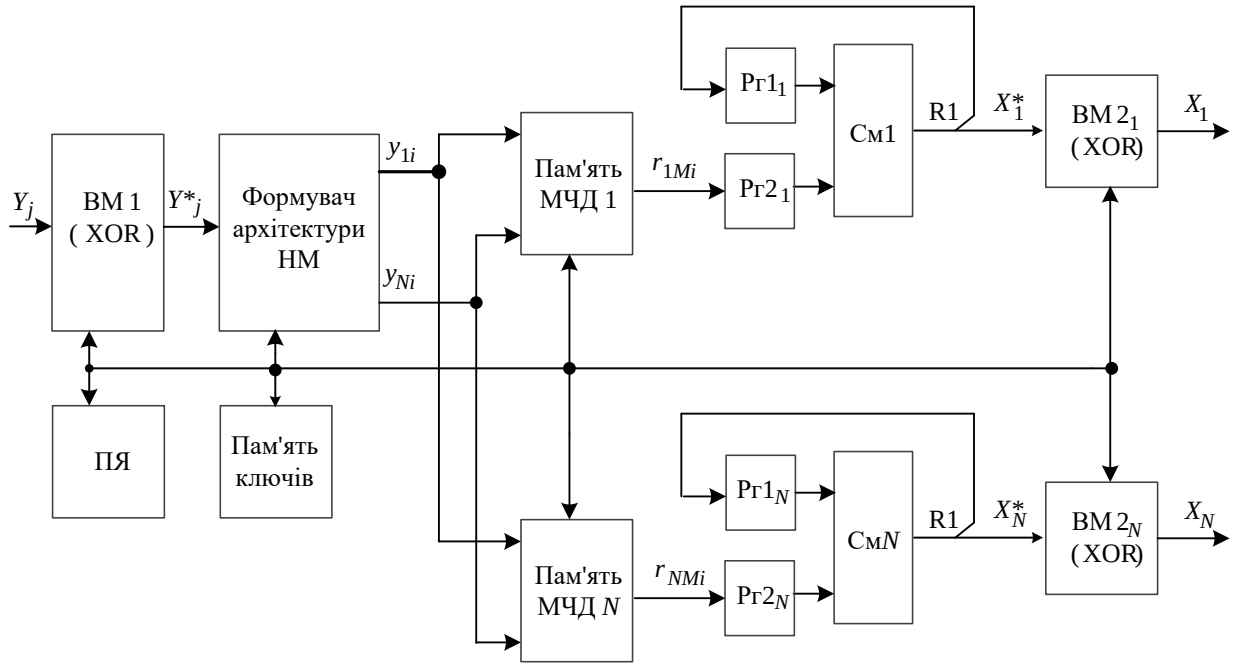

Рис. 2. Структура мобільних засобів нейроподібного криптографічного дешифрування даних: ПЯ – процесорне ядро; ПК – пам'ять ключів; ВМ – вузол маски; ФРЗ – формувач розрядних зрізів; ПМД – пам'ять макрочасткових добутків; ВП – вузол підсумовування

Перед початком дешифрування даних ПЯ задає кількість нейроподібних елементів *N*, вибирає матрицю вагових коефіцієнтів W_j, обчислює таблиці макрочасткових добутків r_{jMi} і записує їх у пам'ять МЧД*j*. Крім того, у вузли ВМ1 і $ВМ2_1$, ..., $ВМ2_N$ записуються вибрані із пам'яті ключів маски. Зашифровані дані Y_j надходять на вхід ВМ1 у форматі із плаваючою комою. Повідомлення з накладеною маскою *X** із виходу ВМ1 надходять на вхід формувача архітектури НМ, де записуються у регістри. На виході формувача архітектури НМ у кожному *i*-му такті отримуємо *i*-й розрядний зріз, який є адресою для читання макрочасткових добутків r_{1Mi},…, r_{NMi} із пам'яті $МЧД_1$, …, $МЧД_N$. У кожному *j*-му такті обчислення скалярного добутку виконується підсумовування макрочасткових добутків r_{jMi} за формулою (6). Обчислені скалярні добутки передаються у вузли $ВМ2_1$, …, $ВМ2_N$, де на них накладається маска. На виходах вузлів $ВМ2_1$, …, $ВМ2_N$ отримують дешифровані дані X_1, …, X_N.

5. Реалізація спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних на FPGA

Проєктування спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних виконано мовою програмування апаратури VHDL у середовищі розроблення Quartus II вер. 13.1 із використанням бібліотек середовища розроблення. Середовище розроблення Quartus II підтримує весь процес проєктування спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних, починаючи із введення проєкту користувачем і завершуючи програмуванням ПЛІС, налагодженням як самої мікросхеми, так і модулів загалом. Основними компонентами спеціалізованих модулів нейроподібного криптографічного шифрування та дешифрування даних є формувач архітектури НМ¸ пам'ять МЧД, тракт обчислення скалярного добутку. Розглянемо проєктування спеціалізованих модулів для випадку, коли повідомлення є восьмирозрядним (m = 8), входів нейромережі чотири (N = 4), а розрядність входів 2 (n = 2).

Порівняння спеціалізованих модулів шифрування та дешифрування даних показує, що складнішими є спеціалізовані засоби модуля дешифрування даних. Тому доцільно розглянути проєктування спеціалізованих засобів модуля дешифрування даних.

Розроблено схему спеціалізованого модуля дешифрування даних, яка наведена на рис. 3.

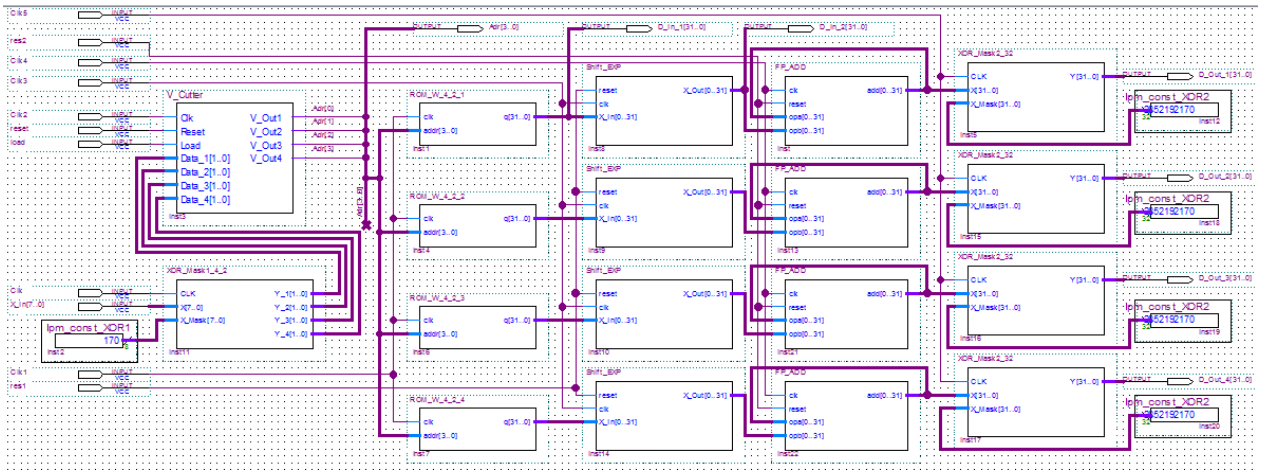

Рис. 3. Схема спеціалізованого модуля дешифрування даних

Особливістю спеціалізованого модуля дешифрування даних є те, що він має чотири нейроподібні елементи, які орієнтовані на роботу із 32-розрядними вхідними даними із плаваючою комою. Вхідні дані In_X0 надходять на вхід блока XOR_Mask2_32. Синхронізація завантаження вхідних даних виконується за переднім фронтом імпульсів Clk_Xor. Вагові коефіцієнти нейроподібних елементів зберігаються у блоках ROM_W_4_2_1_D, …, ROM_W_4_2_4_D. Адреси Adr_Rom для читання вагових коефіцієнтів надходять одночасно на вхід блоків ROM_W_4_2_1_D, …, ROM_W_4_2_4_D. Момент читання даних з таблиць синхронізується за допомогою сигналу *Clk_Gl*. На виході цих блоків отримуємо зчитані з таблиць дані *q*[31..0]. Обчислення скалярних добутків у нейроподібних елементах виконується за допомогою мегафункцій FP_MULT та FP_ADD_SUB. Мегафункція FP_MULT реалізує множення чисел з налаштовуваними параметрами в форматі з плаваючою крапкою. Входи мегафункції: *dataa*[31..0] – множене; *datab*[31..0] – множник; *clk* – імпульси синхронізації. Вихід: *result*[31..0] – добуток вхідних даних. Входи мегафункції FP_ADD_SUB: *dataa*[31..0] – перший доданок або зменшуване; *datab*[31..0] – другий доданок або від'ємник; *clock* – імпульси синхронізації; *aclr* – імпульс скидання виходу мегафункції на нуль. Вихід мегафункції: *result*[31..0] – сума або різниця вхідних даних. На один із входів мегафункції (*dataa*) подається добуток, а на другий (*datab*) заведено обернений зв'язок з її виходу (*result*), що забезпечує обчислення скалярного добутку. Перед кожним початком обчислення скалярного добутку вихід мегафункції обнулюється за допомогою імпульсу *aclr*.

Перетворення отриманих значень на цілі числа виконується за допомогою мегафункції FP_to_INT. Виходи цих мегафункції об'єднуються в один сигнал за допомогою блока XOR_Mask2_8_1. На входи цього блока подаються сигнали Y_1, Y_2, Y_3, Y_4, два молодших байти кожного з них об'єднуються в один вектор розмірністю 8 бітів, на який накладається маска XOR(1). Значення цієї маски передається через вхід X_Mask. Робота цього блока синхронізується тактовими імпульсами Clk_XOR_2. На виході *Out*[7..0] цього блока отримують дешифровані дані.

Часову діаграму моделювання модуля дешифрування наведено на рис. 4.

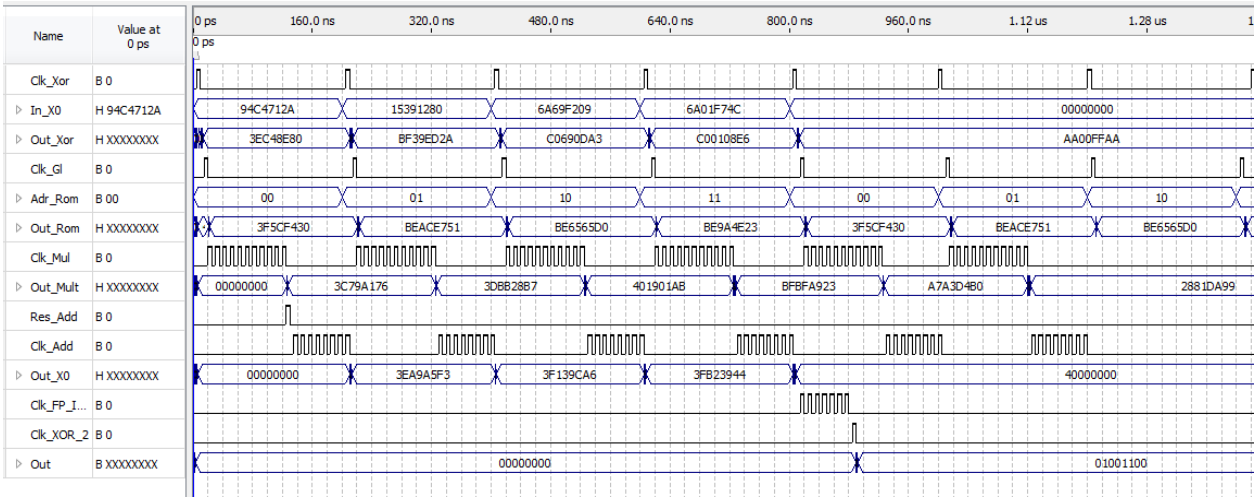

Рис. 4. Часова діаграма моделювання модуля дешифрування

Апаратні ресурси FPGA EP3C16F484C6 сім'ї Cyclone III, які необхідні для реалізації модуля дешифрування, становлять 7357 із 15408 логічних елементів та 5218 регістрів. Час, необхідний на дешифрування одного повідомлення, – приблизно 880 нс.

Висновки

1. Визначено, що проєктування нейроподібних засобів шифрування та дешифрування даних із високою ефективністю використання обладнання зводиться до мінімізації апаратних затрат із забезпеченням множини вимог, характеристик і обмежень.

2. Вдосконалено таблично-алгоритмічний метод обчислення скалярного добутку, який за рахунок приведення до найбільшого спільного порядку вагових коефіцієнтів і формування для них таблиць макрочасткових добутків забезпечує швидке обчислення скалярного добутку для вхідних даних як з фіксованою, так і з плаваючою комою.

3. Розроблено нейроподібні методи шифрування та дешифрування даних у реальному часі, які за рахунок використання багатоопераднього підходу, таблиць макрочасткових добутків і базису елементарних арифметичних операцій забезпечують реалізацію спеціалізованих модулів із високими техніко-економічними показниками.

4. Розроблено на основі універсального процесорного ядра, доповненого спеціалізованими модулями, мобільні засоби нейроподібного криптографічного шифрування та дешифрування даних, які за рахунок взаємопоєднання універсального та спеціалізованого підходів, програмних і апаратних засобів забезпечують ефективну реалізацію алгоритмів криптографічного шифрування та дешифрування даних у реальному часі.

5. Апаратні витрати на реалізацію спеціалізованого модуля нейроподібного криптографічного дешифрування даних (m = 8, n = 2 і N = 4) становлять 7357 логічних елементів та 5218 регістрів, а час, необхідний на дешифрування одного повідомлення, – приблизно 880 нс.

Список літератури

1. Volna, E., Kotyrba, M., Kocian, V., Janosek, M. (2012). Cryptography Based On Neural Network. *Proceedings of the 26th European Conference on Modeling and Simulation,* 386–391.

2. Shihab, K. (2006). A backpropagation neural network for computer network security. *Journal of Computer Science,* Vol. 2, No. 9, 710–715.

3. Sagar, V., Kumar, K. (2014). A Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN). *Proceedings of the 2014 ACM International Conference on Information and Communication Technology for Competitive Strategies*.

4. Arvandi, M., Wu, S., Sadeghian, A., Melek, W. W., Woungang, I. (2006). Symmetric cipher design using recurrent neural networks. *Proceedings of the IEEE International Joint Conference on Neural Networks,* 2039–2046.

5. Цимбал, Ю. В. (2018). Нейромережевий метод симетричного шифрування даних. *Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі*, № 901, 118–122.

6. Tsmots, I., Tsymbal, Y., Skorokhoda, O., Tkachenko, R. (2019). Neural-like methods and hardware structures for real-time data encryption and decryption. *Комп'ютерні науки та інформаційні технології, CSIT-2019: матеріали XIV Міжнар. наук.-техн. конференції*, 17–20 вересня 2019, Львів, Україна, 248–253.

7. Khavalko, V., Tsmots, I. (2019). Image classification and recognition on the base of autoassociative neural network usage. 2019 *IEEE 2nd Ukraine conference on electrical and computer engineering, UKRCON-2019 : conference proceedings* (Lviv, Ukraine, July 2–6, 2019), 1118–1121.

8. Tsmots, I., Rabyk, V., Skorokhoda, O., Teslyuk, T. (2019). Neural element of parallel-stream type with preliminary formation of group partial products. *Electronics and information technologies (ELIT-2019): proceedings of the XIth International scientific and practical conference*, 16–18 September, 2019, Lviv, Ukraine, 154–158.

9. Tsmots, I., Rabyk, V., Skorokhoda, O., Tsymbal, Y. (2021). Neural-like real-time data protection and transmission system. *Advances in Intelligent Systems and Computing (AISC)*, Vol. 1293 : Advances in Intelligent Systems and Computing V. Selected papers from the International conference on computer science and information technologies.

10. Цмоць, І. Г., Лукащук, Ю. А., Хавалко, В. М., Рабик, В. Г. (2019). Моделі нейроподібного елемента паралельно-паралельного типу. *Моделювання та інформаційні технології,* Вип. 86, 119–126.

11. Tsmots, I., Skorokhoda, O., Ignatyev, I., Rabyk, V. (2017). Basic Vertical-Parallel Real Time Neural Network Components. *Proceedings of XIIth International Scientific and Technical Conference CSIT 2017*. 5–8 September 2017. Lviv, Ukraine, 344–347.

12. Цмоць, І. Г., Скорохода, О. В. (2011). Пристрій для обчислення скалярного добутку. Патент України на корисну модель № 66138, бюл. № 24.

13. Цмоць, І. Г., Скорохода, О. В., Теслюк, В. М. (2013). Пристрій для обчислення скалярного добутку. Патент України на винахід № 101922, 13.05.2013, бюл. № 9.

14. Цмоць, І. Г., Скорохода, О. В., Медиковський, М. О. (2019). Пристрій для обчислення скалярного добутку. Патент України на винахід № 118596, 11.02.2019, бюл. № 3.

15. Цмоць, І. Г., Теслюк, В. М., Теслюк, Т. В., Медиковський, М. О., Цимбал, Ю. В. (2019). Пристрій для обчислення сум парних добутків. Патент України № 120210, 25.10.2019, бюл. № 20/2019.

References

1. Volna, E., Kotyrba, M., Kocian, V., Janosek, M. (2012). Cryptography Based On Neural Network. *Proceedings of the 26th European Conference on Modeling and Simulation,* 386–391.

2. Shihab, K. (2006). A backpropagation neural network for computer network security. *Journal of Computer Science*, Vol. 2, No. 9, 710–715.

3. Sagar, V., Kumar, K. (2014). A Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN). *Proceedings of the 2014 ACM International Conference on Information and Communication Technology for Competitive Strategies*.

4. Arvandi, M., Wu, S., Sadeghian, A., Melek, W.W., Woungang, I. (2006). Symmetric cipher design using recurrent neural networks. *Proceedings of the IEEE International Joint Conference on Neural Networks,* 2039– 2046.

5. Tsimbal, Yu. V. (2018). Neural network method of symmetric data encryption. *Bulletin of the Lviv Polytechnic National University. Series: Information systems and networks,* No. 901, 118–122.

6. Tsmots, I., Tsymbal, Y., Skorokhoda, O., Tkachenko, R. (2019). Neural-like methods and hardware structures for real-time data encryption and decryption. *Computer Science and Information Technology,* CSIT-2019*: Proceedings of the XIV International Scientific and Technical Conference*, September 17–20, 2019, Lviv, Ukraine, 248–253.

7. Khavalko, V., Tsmots, I. (2019). Image classification and recognition on the base of autoassociative neural network usage. 2019 IEEE *2-nd Ukraine conference on electrical and computer engineering, UKRCON-2019 : conference proceedings* (Lviv, Ukraine, July 2–6, 2019), 1118–1121.

8. Tsmots, I., Rabyk, V., Skorokhoda, O., Teslyuk, T. (2019). Neural element of parallel-stream type with preliminary formation of group partial products. *Electronics and information technologies (ELIT-2019): proceedings of the XI-th International scientific and practical conference*, 16 –18 September, 2019, Lviv, Ukraine. C. 154–158.

9. Tsmots, I., Rabyk, V., Skorokhoda, O., Tsymbal, Y. (2021). Neural-like real-time data protection and transmission system. Advances in Intelligent Systems and Computing (AISC). Vol. 1293: Advances in Intelligent Systems and Computing V. Selected papers from the International conference on computer science and information technologies.

10. Tsmots, I. G., Lukaschuk, Yu. A., Havalko, V. M, Rabik, V. G. (2019). Models of neuro-like element of parallel-parallel type. *Modeling and information technology*, Vip. 86, 119–126.

11. Tsmots, I., Skorokhoda, O., Ignatyev, I., Rabyk, V. (2017). Basic Vertical-Parallel Real Time Neural Network *Components. Proceedings of XIIth International Scientific and Technical Conference* CSIT 2017. 5–8 September 2017. Lviv, Ukraine, 344–347.

12. Tsmots, I. G., Skorokhoda, O. V. (2011). Device for calculating the scalar product. Patent of Ukraine for utility model No. 66138, bull. No. 24.

13. Tsmots, I. G., Skorokhoda, O. V., Teslyuk, V. M. (2013). Device for calculating the scalar product. Patent of Ukraine for the invention No. 101922, 13.05.2013 bull. No. 9.

14. Tsmots, I. G., Skorokhoda, O. V., Medikovsky, M. O. (2019). Device for calculating the scalar product. Patent of Ukraine for the invention No. 118596, 11.02.2019, bull. No. 3.

15. Tsmots, I. G., Teslyuk, V. M, Teslyuk, T. V, Medikovsky, M. O, Tsymbal, Y. V. (2019). Device for calculating the sums of paired products. Patent of Ukraine No. 120210, 25.10.2019, bull. No. 20/2019.

DEVELOPMENT OF MOBILE FACILITIES OF NEURO-LIKE CRYPTOGRAPHIC ENCRYPTION AND DECRYPTION OF DATA IN REAL TIME

Ivan Tsmots [1], Vasyl Rabyk [2], Yurii Lukashchuk [3]

[1, 3] Lviv Polytechnic National University

[2] Lviv National University of Ivan Franko

[1] ivan.tsmots@gmail.com, ORCID 0000-0002-4033-8618

[2] vasyl.rabyk@lnu.edu.ua, ORCID 0000-0003-2655-0812

[3] urijlukas@gmail.com, ORCID 0000-0002-8933-8635

The requirements are formed, the method is chosen and the main stages of development of mobile means of neuro-like cryptographic encryption and real-time data decryption are considered. It is shown that the development of mobile means of neuro-like cryptographic encryption and decryption of real-time data with high efficiency of equipment is reduced to minimize hardware costs while providing a variety of requirements, characteristics and limitations. The tabular-algorithmic method of calculating the scalar product has been improved. Namely, the ability to work with floating-point operands has been added and it is focused on hardware and software implementation. Developed on the basis of a universal processor core, supplemented by specialized modules, mobile means of neuro-like cryptographic encryption and data decryption. Which due to the combination of universal and specialized approaches, software and hardware provides effective implementation of algorithms for cryptographic encryption and decryption of data in real time. It is proposed to use a multioperand approach, tables of macroparticle products and bases of elementary arithmetic operations to achieve high technical and economic indicators in the implementation of specialized modules of neuro-like cryptographic encryption and real-time data decryption. Specialized modules of neuro-like cryptographic encryption and data decryption have been implemented using the VHDL hardware programming language and the Quartus II development environment (version 13.1) on the FPGA. The evaluation of hardware and time parameters of the developed specialized module of neurosimilar cryptographic data decryption is carried out.

Key words: data encryption; data decryption; neural network; scalar product; specialized module; neuro-like element; FPGA.