DOI: https://doi.org/10.33216/1998-7927-2025-296-10-5-12

УДК 004.94:655.1

АДАПТИВНА СИМЕТРИЧНА КРИПТОСИСТЕМА З ДИНАМІЧНИМ УЗГОДЖЕННЯМ КЛЮЧІВ НА ОСНОВІ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ

Множинський Б.Г.

ADAPTIVE SYMMETRIC CRYPTOSYSTEM WITH DYNAMIC KEY AGREEMENT BASED ON DEEP NEURAL NETWORKS

Mnozhynskyi B.H.

Стаття присвячена розробці адаптивної симетричної криптосистеми. Формування ключів відбувається без традиційних протоколів обміну. Метод базується на синхронізації глибоких нейронних мереж. Процес реалізується через відкритий канал зв'язку. Мета роботи полягає в обґрунтуванні нової архітектури забезпечення динамічного управління в просторої нейронних мереж. Механізм ґрунтується на нейронній синхронізації. Оцінюється криптографічна стійкість та обчислювальна ефективність моделі. Методологія інтегрує криптографічний аналіз та теорію нейронних мереж. Застосовано формалізований опис алгоритмічних конструкцій. Виконано аналітичне оцінювання обчислювальної складності. Проведено порівняння з класичними схемами симетричного шифрування. Результатом є архітектура з децентралізованою логікою узгодження ключів. Ключ формується як функція внутрішнього стану мережі. Алгоритм охоплює ініціалізацію, синхронізацію та генерацію ключів. Система забезпечує циклічне оновлення ключового матеріалу. Реалізовано процедури шифрування та дешифрування. Проведено аналіз стійкості до пасивних атак. Досліджено резистентність до активних форм втручання. Система протидіє атакам перехоплення та інжекції. Механізм захищає від атак посередницького типу. Адаптивність моделі знижує кореляцію між послідовними ключами. Реконструкція внутрішніх станів суттєво ускладнюється. Обчислювальна складність залишається прийнятною для практичного застосування. Нейронна компонента не знижує продуктивність системи за тривалих комунікаційних сеансів. Практична цінність полягає у застосуванні в розподілених мережах. Система функціонує без централізованої інфраструктури довіри. Результати придатні для вбудованих обчислювальних систем. Підхід застосовний у мобільних та сенсорних мережах. Модель зменшує залежність від асиметричної криптографії. Елімінуються пікові обчислювальні навантаження. Перспективи пов'язані з експериментальною верифікацією на апаратних платформах. Планується поглиблений аналіз стійкості до комбінованих векторів атак. Окремий науковий інтерес становить оптимізація архітектурних рішень.

Ключові слова: *адаптивна криптосистема, симетричне шифрування, динамічне узгодження ключів, глибокі нейронні мережі, нейронна синхронізація, криптографічна стійкість.*

Вступ. Розвиток мережевих систем передавання даних супроводжується зростанням вимог до криптографічного захисту за умов відкритих каналів, обмежених ресурсів і мінливої структури загроз. Симетричні криптосистеми зберігають високу обчислювальну ефективність, проте їхня практична безпека істотно залежить від способу формування, узгодження та оновлення ключів. Традиційні підходи до керування ключами спираються на попередній розподіл секретів або на асиметричні протоколи, які створюють додаткові часові, енергетичні та організаційні витрати, а також формують уразливі точки при компрометації початкових параметрів. Окремою проблемою є статичний характер ключового матеріалу у більшості симетричних схем. Фіксований або рідко оновлюваний ключ підвищує ефективність пасивного аналізу, спрощує кореляційні атаки та зменшує стійкість

системи в тривалих сеансах обміну [18]. Навіть за достатньої довжини ключа зберігається ризик поступового накопичення інформації про його структуру.

За цих умов і актуалізується потреба в криптографічних механізмах, які поєднують ефективність симетричного шифрування з динамічними процесами формування секретів. Особливий інтерес становлять підходи, що не використовують класичні протоколи обміну ключами, а формують спільний секрет у процесі адаптивної взаємодії сторін. Постановка проблеми дослідження полягає у розробці та обґрунтуванні симетричної криптосистеми, в якій узгодження та оновлення ключів реалізуються як керований динамічний процес на основі глибоких нейронних мереж, з забезпеченням криптографічної стійкості, прийнятної обчислювальної складності та практичної придатності для розподілених інформаційних середовищ.

Метою статті є наукове обґрунтування використання адаптивної симетричної криптосистеми, у якій узгодження і регулярне оновлення криптографічних ключів реалізуються як динамічний процес синхронізації глибоких нейронних мереж.

Виклад основного матеріалу дослідження. Адаптивна симетрична криптосистема ґрунтується на принципі безперервної зміни криптографічних параметрів у процесі сеансу зв'язку. Система орієнтована на мінімізацію статичних елементів, які формують передбачуваність для зловмисника. Центральним елементом виступає динамічний механізм узгодження ключів, інтегрований безпосередньо у логіку симетричного шифрування. Архітектура системи має децентралізований характер. Кожна сторона обміну діє автономно, без залучення довіреного центру або сервера керування ключами для усунення точки єдиного компрометаційного ризику. Архітектурна модель включає модуль шифрування, модуль нейронної синхронізації, модуль адаптації параметрів та модуль контролю цілісності станів. Сторони обміну виконують симетричні функції [2]. Кожен учасник підтримує ідентичну нейронну структуру, однакові правила оновлення ваг і спільно визначені початкові обмеження параметрів. Відсутність функціональної асиметрії знижує ризик витоку службової інформації через поведінкові відмінності протоколу.

Комунікація між сторонами здійснюється через відкритий канал. Передаються лише допоміжні сигнали синхронізації, які не містять безпосередньої інформації про значення ключа. Захищений канал на початковому етапі не потрібен. Це розширює можливості застосування системи в умовах обмеженої інфраструктури або в динамічних мережах. Криптографічний ключ не зберігається у статичному вигляді. Він існує як поточний стан узгодженої нейронної моделі. Будь-яка спроба перехоплення фіксує лише часткові сигнали, непридатні для відновлення внутрішнього стану системи [16]. Таким чином, криптосистема реалізує принцип еволюційної секретності. Адаптивність архітектури проявляється у здатності змінювати параметри нейронної моделі залежно від характеристик каналу, інтенсивності трафіку та часових обмежень. Система реагує на зовнішні впливи не шляхом аварійного завершення сеансу, а шляхом перебудови внутрішніх станів.

Модель динамічного узгодження ключів базується на синхронізації глибоких нейронних мереж між сторонами обміну. Узгодження відбувається без передачі самих ваг або ключових значень. Процес реалізує спільну еволюцію станів на основі однакових вхідних стимулів та узгоджених правил навчання. Нейронна мережа має багаторівневу структуру. Вхідний шар формує випадкові або псевдовипадкові вектори стимулів. Приховані шари забезпечують нелінійне перетворення сигналів та підвищують ентропію внутрішнього представлення. Вихідний шар генерує бінарні або дискретні сигнали синхронізації. Глибина мережі визначає рівень криптографічної стійкості. Зі збільшенням кількості шарів зростає складність реконструкції внутрішнього стану навіть за наявності повного журналу переданих сигналів [19]. При цьому зберігається можливість синхронізації між легітимними сторонами. Процес синхронізації має ітеративний характер. На кожному кроці сторони обробляють однаковий вхідний вектор, обмінюються вихідними сигналами та коригують ваги згідно з локальним правилом навчання.

Синхронізація досягається після збігу внутрішніх станів з наперед заданою точністю. Адаптація параметрів реалізується через зміну швидкості навчання, діапазонів ваг та частоти оновлення. Механізм адаптації активується при виявленні аномалій у каналі або зміні режиму навантаження. Це забезпечує стабільність

синхронізації без зниження рівня секретності. Ключ формується як детермінована функція поточного стану нейронної мережі. Він не передається каналом і не зберігається після завершення сеансу. Зміна хоча б одного параметра мережі призводить до повної декореляції ключового простору [6]. Для оцінювання практичних характеристик моделі доцільно розглядати систему параметрів, що впливають на безпеку, продуктивність та стійкість синхронізації (табл. 1).

Представлена модель не потребує класичних протоколів обміну ключами. Вона замінює їх процесом спільної адаптивної еволюції, що знижує залежність від математичних припущень, характерних для традиційної криптографії [4]. Стійкість моделі визначається не лише розміром ключового простору, а й складністю відтворення динаміки навчання. Зловмисник стикається з необхідністю одночасного відновлення структури мережі, параметрів адаптації та початкових умов. Алгоритм роботи адаптивної симетричної криптосистеми формує замкнений цикл, у межах якого ініціалізація, узгодження, шифрування та оновлення ключів відбуваються без фіксованих статичних станів. Криптографічна логіка інтегрується з механізмами нейронної адаптації, тому кожен етап алгоритму впливає на наступний. Процес ініціалізації визначає початкову допустиму область параметрів. Сторони обміну погоджують структуру нейронної мережі, кількість шарів, розмірність вхідних векторів та правила корекції ваг [8]. Початкові значення ваг не збігаються, але обмежуються однаковими інтервалами. Формально початковий стан мережі кожної сторони задається як:

$$W^{(o)} = \left\{ w_{ij} \mid w_{ij} \in [-\alpha,\ \alpha] \right\}, \qquad (1)$$

де: α – граничний діапазон допустимих значень. Вибір α впливає на швидкість синхронізації та рівень ентропії внутрішніх станів.

Генерація вхідних стимулів відбувається на кожній ітерації синхронізації. Вхідний вектор X^t формується як псевдовипадкова послідовність:

$$X^t = \left\{ x_1^t,\ x_2^t,\ \ldots,\ x_n^t \right\}, x_i^t \in \{-1, +1\}, \qquad (2)$$

Надані вектори можуть генеруватися детерміновано на основі лічильника або спільного початкового зерна. Передача X^tвідкритим каналом не знижує рівень секретності, оскільки без знання внутрішніх ваг нейронної мережі відновлення стану неможливе. Вихід нейронної мережі визначається як функція активації [7]:

$$y^t = sign\left(\sum w_j^t \cdot x_j^t \right). \qquad (3)$$

Сторони обмінюються лише значенням y^t. За умови збігу вихідних сигналів активується правило навчання. Оновлення ваг здійснюється за локальним детермінованим алгоритмом:

$$w_j^{t+1} = w_j^t + \eta \cdot x_j^t \, y^t. \qquad (4)$$

де η є коефіцієнтом адаптації. Зміна η у часі дозволяє керувати компромісом між швидкістю синхронізації та стійкістю до атак спостереження. Ключ симетричного шифрування формується як функція поточного стану мережі:

Таблиця 1

Практичні параметри моделі динамічного узгодження ключів на основі глибокої нейронної мережі [5; 13]

Параметр моделі	Функціональне призначення	Вплив на стійкість	Вплив на швидкодію	Практичні обмеження
Кількість прихованих шарів	Формування глибокого внутрішнього представлення	Зростання простору атак	Збільшення часу синхронізації	Обчислювальні ресурси
Розмір вектору стимулів	Визначення ентропії вхідних даних	Зниження кореляцій	Помірний вплив	Пропускна здатність каналу
Діапазон ваг	Контроль варіативності станів	Ускладнення відновлення	Незначний вплив	Чутливість до шуму
Швидкість навчання	Регулювання темпу синхронізації	Баланс стійкості і стабільності	Прямий вплив	Ризик розсинхронізації
Частота оновлення ключа	Обмеження часу дії ключа	Зменшення вікна атаки	Додаткові обчислення	Затримки в реальному часі

$$K^t = H\left(W^t\right). \quad (5)$$

де H є криптографічною хеш-функцією або бієктивним перетворенням, що забезпечує рівномірний розподіл ключового простору.

Таким чином, ключ існує лише у похідному вигляді і не збігається безпосередньо з вагами мережі. Оновлення ключів відбувається або після фіксованої кількості блоків, або після досягнення заданого порогу дивергенції каналу [10]. Частота оновлення описується як:

$$f_k = \frac{B}{T}. \quad (6)$$

де B кількість зашифрованих блоків;

T це час сеансу.

Збільшення f_k зменшує часовий інтервал ефективної атаки.

Процедура шифрування використовує стандартний симетричний примітив, наприклад, блоковий шифр у режимі потокової модифікації. Шифротекст C_i формується як:

$$C_i = E\left(P_i, K_t\right), \quad (7)$$

де P_i є відкритим блоком даних. Дешифрування виконується симетрично:

$$P_i = D\left(C_i, K^t\right). \quad (8)$$

У разі втрати синхронізації система не припиняє роботу. Активується повторна фаза узгодження, що дозволяє відновити коректний стан без втрати конфіденційності попередніх блоків (табл. 2).

Криптографічна стійкість адаптивної симетричної криптосистеми визначається сукупністю динамічних та структурних факторів. На відміну від класичних схем, оцінювання безпеки не зводиться до розміру ключа або складності окремої математичної задачі. Пасивна атака передбачає спостереження за відкритим каналом без втручання у протокол. Зловмисник отримує доступ до послідовностей X^t та y^t. Для відновлення ключа необхідно реконструювати внутрішній стан нейронної мережі, що формально зводиться до задачі з експоненційною складністю [1]:

$$P\left(recover\ W \mid X, y\right) \to 0\ при\ n \to \infty. \quad (9)$$

де n є розмірністю вхідного простору. Зі зростанням глибини мережі простір можливих конфігурацій ваг зростає надлінійно.

Активні атаки передбачають модифікацію переданих сигналів або інжекцію власних значень y^t. У таких умовах алгоритм адаптації призводить до розсинхронізації атакуючої сторони з легітимними учасниками. Будь-яке неконсистентне втручання порушує правило навчання та призводить до випадкової еволюції станів [11].

Стійкість до атаки типу «людина посередині» зумовлена відсутністю фіксованих секретів. Атакуючий агент не здатний підтримувати одночасну синхронізацію з обома сторонами, оскільки адаптація параметрів залежить від локального стану кожного вузла. Адаптивність системи підвищує рівень безпеки шляхом зміни статистичних властивостей ключового потоку. Навіть у разі часткового витоку інформації кореляція між послідовними ключами мінімізується:

$$corr\left(K^t, K^{t+1}\right) \approx 0. \quad (10)$$

Цей крок виключає можливість екстраполяції ключів на основі попередніх значень (табл. 3).

Таблиця 2

Алгоритмічні етапи роботи адаптивної симетричної криптосистеми (сформовано автором)

Етап алгоритму	Вхідні дані	Основні операції	Вихідні дані	Криптографічний ефект
Ініціалізація	Структура мережі, α	Генерація початкових ваг	$W^{(0)}$	Формування початкової ентропії
Синхронізація	X^t, y^t	Оновлення ваг	W^t	Узгодження станів
Генерація ключа	W^t	Хешування	K^t	Отримання симетричного ключа
Шифрування	P_i, K^t	Блокове перетворення	C_i	Конфіденційність
Оновлення ключа	Лічильник, канал	Адаптація параметрів	K^{t+1}	Обмеження часу дії ключа

Таблиця 3

Стійкість адаптивної симетричної криптосистеми до типових класів атак (сформовано автором)

Тип атаки	Доступ атакуючого	Механізм протидії	Результат атаки
Пасивне спостереження	X^t, y^t	Висока ентропія станів	Відновлення ключа неможливе
Активна інжекція	Модифікація y^t	Розсинхронізація	Втрата контролю атакуючим
Повтор сигналів	Архів трафіку	Адаптивне оновлення	Некоректні ключі
Людина посередині	Повний контроль каналу	Локальна адаптація	Неможливість синхронізації

Вплив адаптивності на безпеку проявляється у зменшенні предиктивності системи. Криптосистема перестає бути стаціонарною. Це ускладнює формування універсальних атакуючих стратегій. Безпека системи визначається не одноразовою складністю, а стійкістю процесу еволюції у часі. Обчислювальна ефективність адаптивної симетричної криптосистеми визначається сукупною вартістю нейронної синхронізації, генерації ключів та симетричних криптографічних перетворень [12]. На відміну від класичних схем, часові витрати тут розподіляються динамічно протягом усього сеансу, а не концентруються на одноразовій процедурі обміну ключами (рис. 1).

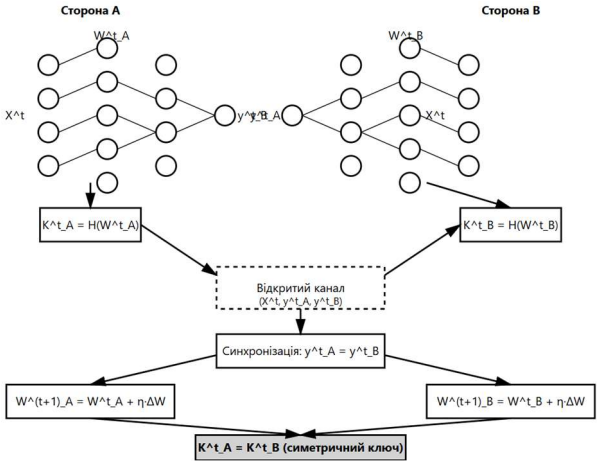

Рис. 1. Схема адаптивної криптосистеми на основі нейронної мережі (побудовано автором)

Основним джерелом додаткових обчислювальних витрат виступає процес синхронізації глибоких нейронних мереж. Нехай L є кількістю шарів мережі, N є кількістю нейронів у шарі, T_s є кількістю ітерацій синхронізації. Тоді асимптотична обчислювальна складність одного повного циклу узгодження оцінюється як:

$$C_s = O\left(T_s \cdot L \cdot N^2\right). \tag{11}$$

де N^2 відображає операції зваженого підсумовування між нейронами суміжних шарів. Зростання L підвищує криптографічну стійкість, але лінійно збільшує часові витрати.

Час синхронізації є стохастичною величиною. Його математичне сподівання залежить від діапазону початкових ваг α та коефіцієнта адаптації η [9]. Очікувана кількість ітерацій досягнення синхронного стану може бути описана як:

$$E\left[T_s\right] \approx \frac{k \cdot \alpha^2}{\eta}, \tag{12}$$

де k є емпіричним коефіцієнтом, що залежить від архітектури мережі.

Зменшення показника η знижує швидкість навчання, але стабілізує процес синхронізації. Генерація ключа є похідною операцією. Якщо ключ формується через хешування стану ваг, то його обчислювальна складність визначається складністю хеш-функції:

$$C_k = O\left(|W|\right). \tag{13}$$

де $|W|$ є кількістю параметрів нейронної мережі. За умови фіксованої архітектури ця величина залишається сталою для кожного оновлення ключа.

Процедури шифрування та дешифрування базуються на стандартних симетричних перетвореннях [15]. Для блокового шифру з розміром блоку b та довжиною повідомлення M часові витрати описуються як:

$$C_e = O\left(\frac{M}{b}\right), \tag{14}$$

Описана складова не залежить від нейронної частини системи і збігається за порядком з класичними симетричними схемами [3]. Сумарні часові витрати за один сеанс зв'язку визначаються як:

$$C_{total} = C_s + n \cdot C_k + C_e. \quad (15)$$

де n_k є кількістю оновлень ключа за сеанс. За великих обсягів переданих даних частка C_e домінує, а відносний внесок нейронної синхронізації зменшується.

Продуктивність системи, краще за все, оцінювати через пропускну здатність. Нехай τ_e є середнім часом шифрування одного блоку, τ_s є середнім часом ітерації синхронізації. Тоді ефективна пропускна здатність визначається як:

$$P_{eff} = \frac{M}{\left(T_s \cdot \tau_s + M \cdot \tau_e\right)}. \quad (16)$$

За умови рідкісного оновлення ключів та великих повідомлень P_{eff} наближається до пропускної здатності класичного симетричного шифру. Порівняння з класичними схемами доцільно проводити з урахуванням фазової структури криптографічних протоколів. У традиційних симетричних системах обмін ключами реалізується або через попередньо розподілений секрет, або через асиметричні алгоритми [14]. Часова складність асиметричного узгодження ключів може бути оцінена як:

$$C\_RSA = O\left(n^3\right) \quad (17)$$

де n є розміром модуля.

Сформована операція виконується одноразово, але створює значні затримки при коротких сесіях. Для схем на основі еліптичних кривих складність однієї операції множення точки оцінюється як:

$$C\_ECC = O\left(n^2\right) \quad (18)$$

що є меншим, але все одно перевищує складність однієї ітерації нейронної синхронізації за помірних значень N. Головна відмінність полягає у часовому розподілі навантаження. Класичні схеми концентрують складні операції на початку сеансу. Адаптивна симетрична криптосистема розподіляє витрати рівномірно у часі. Це знижує пікові затримки та підвищує стабільність продуктивності. Цінним показником стає енергетична вартість обчислень [17]. Нехай E_{op} є середнім енергоспоживанням однієї арифметичної операції. Тоді енергетичні витрати синхронізації описуються як:

$$E_s = Eop \cdot T_s \cdot L \cdot N^2. \quad (19)$$

Для вбудованих пристроїв виданий показник критичний. Проте відсутність асиметричних операцій з великими числами компенсує додаткові витрати на нейронну частину. Масштабованість системи визначається залежністю C_s від параметрів мережі. Збільшення N покращує криптографічні властивості, але квадратично впливає на складність. Тому практичні реалізації орієнтуються на компромісні значення N, за яких досягається баланс між безпекою та продуктивністю. Чутливість продуктивності до частоти оновлення ключів описується як:

$$C_k = \frac{\partial C\_total}{\partial n_k}, \quad (20)$$

Це означає, що надмірно часте оновлення ключів лінійно збільшує сумарні витрати, але не впливає на складність шифрування. Для потокових сценаріїв передавання даних доцільно обмежувати n_k таким чином, щоб виконувалась нерівність:

$$C_s + n_k \cdot C_k \square \ C_e. \quad (21)$$

Наведена умова гарантує нам, що нейронна складова не знижує загальну пропускну здатність системи. Таким чином, обчислювальна складність адаптивної симетричної криптосистеми має керований характер. Вона визначається параметрами архітектури та режимом роботи, а не жорстко зафіксованими криптографічними операціями. У порівнянні з класичними схемами система демонструє нижчі пікові затримки, відсутність дорогих асиметричних операцій та прогнозовану продуктивність у тривалих сесіях зв'язку.

Висновки. Дослідження доводить доцільність відмови від класичних протоколів обміну ключами у симетричних криптосистемах шляхом переходу до динамічного формування ключового матеріалу. Узгодження ключів через нейронну синхронізацію переводить процес захисту з площини статичних секретів у площину керованої еволюції станів. Такий підхід змінює саму логіку криптографічної

безпеки, оскільки компрометація окремих повідомлень або службових сигналів не надає атакуючому достатньої інформації для відновлення секрету, а часовий фактор стає додатковим елементом захисту.

Запропонована архітектура показала здатність протидіяти як пасивним, так і активним загрозам без залучення централізованої інфраструктури довіри. Відсутність фіксованого ключа та постійна перебудова внутрішніх параметрів унеможливлюють ефективні атаки спостереження, інжекції та посередництва. Криптографічна стійкість формується не лише розміром ключового простору, а й складністю відтворення динаміки нейронного навчання, що суттєво ускладнює побудову універсальних атакуючих стратегій. Аналіз обчислювальної складності підтвердив практичну придатність адаптивної симетричної криптосистеми для тривалих сеансів зв'язку. Розподілений у часі характер нейронних обчислень знижує пікові навантаження та усуває дорогі асиметричні операції. За великих обсягів передавання даних продуктивність системи наближається до показників класичних симетричних схем, що відкриває можливості використання запропонованого підходу у вбудованих, мобільних і сенсорних мережах.

Література

1. Abrar A., Dasgupta S., Rahman M., Alsharif A. AI-driven post-quantum cryptography for cyber-resilient V2X communication in transportation cyber-physical systems. arXiv. 2025. https://doi.org/10.48550/arXiv.2510.08496
2. Alanazi M. J., Alhoweiti R. A., Alhwaity G. A., Alharbi A. R. An adaptive hybrid cryptographic framework for resource-constrained IoT devices. Electronics. 2025. Vol. 14. No. 23. Article 4666. https://doi.org/10.3390/electronics14234666
3. Alzaidy S., Binsalleeh H. Adversarial attacks with defense mechanisms on convolutional neural networks and recurrent neural networks for malware classification. Applied Sciences. 2024. Vol. 14. No. 4. Article 1673. https://doi.org/10.3390/app14041673
4. Bhat R., Nanjundegowda R. Exploring generative adversarial networks for secure data encryption and future directions in communication systems. Proceedings of the International Conference on Futuristic Technology. 2025. https://doi.org/10.5220/0013591300004664
5. Geng Y. Identification of cryptosystem based on deep neural network. Highlights in Science, Engineering and Technology. 2025. Vol. 142. p. 391–399. https://doi.org/10.54097/zfm1nx90
6. Hanafi B., Bokhari M. U., Wani M. A., Shakil K. A., Ali G. Dynamic adversarial neural cryptography for ensuring privacy in smart contracts. PeerJ Computer Science. 2025. Vol. 11. Article e3286. https://doi.org/10.7717/peerj-cs.3286
7. Hao J., Jin M., Li Y., Yang Y. Neural network-based symmetric encryption algorithm with encrypted traffic protocol identification. PeerJ Computer Science. 2025. Vol. 11. Article e2750. https://doi.org/10.7717/peerj-cs.2750
8. He Z., Sayadi H. AI in chaos: Adaptive and secure communication via deep reinforcement learning and moving target defense. IEEE Access. 2025. Vol. 13. p. 199971–200000. https://doi.org/10.1109/ACCESS.2025.3635665
9. Jain K. Exploring cryptographic key management schemes for enhanced security in WSNs. Journal of Information and Applied Science. 2025. Vol. 20. No. 1. p. 18–37. https://doi.org/10.2478/ias-2025-0002
10. Jung I. S., Song Y. R., Jilcha L. A., Kim D. H., Im S. Y., Shim S. W., Kim Y. H., Kwak J. Enhanced encrypted traffic analysis leveraging graph neural networks and optimized feature dimensionality reduction. Symmetry. 2024. Vol. 16. No. 6. Article 733. https://doi.org/10.3390/sym16060733
11. Koshiba T., Zolfaghari B., Bibak K. A tradeoff paradigm shift in cryptographically-secure pseudorandom number generation based on discrete logarithm. Journal of Information Security and Applications. 2023. Vol. 73. Article 103430. https://doi.org/10.1016/j.jisa.2023.103430
12. Kumar P. R., Goel S. A secure and efficient encryption system based on adaptive and machine learning for securing data in fog computing. Scientific Reports. 2025. Vol. 15. Article 11654. https://doi.org/10.1038/s41598-025-92245-9
13. Makedon V. V., Kholod O. H., Yarmolenko L. I. The model for assessing the competitiveness of high tech enterprises on the basis of the formation of key competences. Academic Review. 2023. Vol. 59. No. 2. p. 75–89. https://doi.org/10.32342/20745354-2023-2-59-5
14. Makedon V., Myachin V., Aloshyna T., Cherniavska I., Karavan N. Improving the readiness of enterprises to develop sustainable innovation strategies through fuzzy logic models. Economic Studies (Ikonomicheski Izsledvania). 2025. Vol. 34. No. 5. p. 165–179. URL: https://archive.econ-studies.iki.bas.bg/2025/2025_05/2025_05_09.pdf
15. Mohsin Z. R. AI-powered encryption revolutionizing cybersecurity with adaptive cryptographic algorithms. Turkish Journal of Computer and Mathematics Education. 2025. Vol. 16. No. 1. p. 44–62. https://doi.org/10.61841/turcomat.v16i1.14976
16. Reddy P. S., Reddy T. S., Khaled M. K. Enhanced steganography using dynamic compression and

encryption algorithms. International Journal of Engineering Innovations and Management Strategies. 2025. Vol. 1. No. 3. p. 1–13.
17. Saha A., Pathak C., Saha S. A study of machine learning techniques in cryptography for cybersecurity. American Journal of Electronics & Communication. 2021. Vol. 1. No. 4. p. 22–26.
18. Singh M., Baranwal N., Singh K. N., Singh A. K. Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network. IEEE Transactions on Consumer Electronics. 2023. Vol. 70. No. 1. p. 3977–3984. https://doi.org/10.1109/TCE.2023.3276732
19. Zarei M., Dindarlou M. H. F., Taghizadeh M., et al. Lightweight image encryption for wireless sensor networks using optimized elliptic curve and fuzzy logic. Scientific Reports. 2025. https://doi.org/10.1038/s41598-025-32877-z

Mnozhynskyi B.H. Adaptive symmetric cryptosystem with dynamic key agreement based on deep neural networks

The article is devoted to the development of an adaptive symmetric cryptosystem. Key formation is performed without traditional key exchange protocols. The method is based on the synchronization of deep neural networks. The process is implemented over an open communication channel. The purpose of the study is to substantiate a new architecture for dynamic key management in the space of neural networks. The mechanism relies on neural synchronization. Cryptographic robustness and computational efficiency of the model are evaluated. The methodology integrates cryptographic analysis and neural network theory. A formalized description of algorithmic constructions is applied. An analytical assessment of computational complexity is carried out. A comparison with classical symmetric encryption schemes is performed. The result is an architecture with decentralized key agreement logic. The key is generated as a function of the internal state of the network. The algorithm covers initialization, synchronization, and key generation. The system provides cyclic updating of key material. Encryption and decryption procedures are implemented. Resistance to passive attacks is analyzed. Robustness against active forms of interference is investigated. The system counteracts interception and injection attacks. The mechanism protects against man-in-the-middle attacks. Model adaptivity reduces correlation between successive keys. Reconstruction of internal states is significantly complicated. Computational complexity remains acceptable for practical application. The neural component does not reduce system performance during long communication sessions. Practical value lies in application within distributed networks. The system operates without centralized trust infrastructure. The results are suitable for embedded computing systems. The approach is applicable to mobile and sensor networks. The model reduces dependence on asymmetric cryptography. Peak computational loads are eliminated. Future work is associated with experimental verification on hardware platforms. An in-depth analysis of resistance to combined attack vectors is planned. A separate scientific interest concerns optimization of architectural solutions.

Keywords: *adaptive cryptosystem, symmetric encryption, dynamic key agreement, deep neural networks, neural synchronization, cryptographic robustness.*

Множинський Богдан Георгійович – аспірант, Київський Національний Університет Технологій Та Дизайну (Київ), mnbogdan98@gmail.com

Стаття подана 12.11.2025.