УДК 004.8+004.056

Л. М. Куперштейн
А. Є. Татарчук

АНАЛІЗ АКТУАЛЬНОСТІ ЗАСТОВУАННЯ НЕЙРОННИХ МЕРЕЖ В БЛОКОВИХ ШИФРАХ

Вінницький національний технічний університет

Анотація
Розглядається актуальність застосування штучних нейронних мереж в блокових шифрах.
Ключові слова: штучна нейронна мережа, блоковий шифр.

Abstract
The urgency of application of artificial neural networks in block ciphers is considered.
Keywords: artificial neural network, block cipher.

Вступ

За останні кілька років спостерігається підвищення інтересу до нейронних мереж, які успішно застосовуються в різних областях – бізнесі, медицині, техніці, геології, фізики. Нейронні мережі увійшли в практику всюди, де потрібно вирішувати завдання прогнозування, класифікації або правління. Класичні криптографічні алгоритми засновані на складності математичних проблем обчислювальної алгебри, теорії ймовірності, теорії чисел і т.д. Їх основна мета - забезпечення можливості взаємодії через незахищений канал зв'язку. Альтернативним варіантом може стати застосування штучних нейронних мереж, які завдяки своїй гнучкості і можливостям апроксимації здатні вирішувати найрізноманітніші завдання.

Метою роботи є оцінка актуальності використанням штучних нейронних мереж в блокових шифрах.

Результати дослідження

Проблема захисту інформації шляхом її перетворення, що виключає її прочитання сторонньою особою, завжди була важливим завданням. В даний час використання криптографічних методів в інформаційних системах стало особливо актуальним [1].

З одного боку, розширилося використання комп'ютерних мереж, зокрема глобальної мережі Інтернет, по яких передаються великі обсяги інформації державного, військового, комерційного і приватного характеру, що не допускає можливість доступу до неї сторонніх осіб.

З іншого боку, через процес постійного зростання обчислювальних потужностей сучасних комп'ютерів, а також технологій мережевих і нейронних обчислень зробило можливим дискредитацію криптографічних систем, які ще нещодавно вважалися практично не зламними.

Таким чином, актуально шукати нові підходи до вирішення даного завдання – наприклад, нейромережевий підхід – це одна з нових ідей для побудови криптографічних систем [2, 3].

Нейрокриптографія – це область криптографії, призначена для аналізу застосування стохастичних алгоритмів, особливо нейромережевих алгоритмів, для використання в шифруванні і криптоаналізі [2].

Модель штучної нейронної мережі підходить для задач шифрування. В роботі [4] автор спробував реалізувати Rijndael-криптосистему за допомогою штучних нейронних мереж. Ця криптосистема має менш складну будову, ніж AES і не лінійна в експлуатації. Нелінійної повинна бути нейронна мережа зі зворотним зв'язком, що дозволило б виконати шифрування / розшифрування відкритого тексту, зашифрованого тексту з високою продуктивністю і дуже низьким рівнем помилок. Ідея автора полягала в тому, щоб розробити таку нелінійну штучних нейронних мереж. Зменшення ймовірності зламу досягається за допомогою нелінійної функції активації, також властивість нелінійної апроксимації

мережі є корисним для практичного застосування.

В статті [5] пропонується метод формування ключів для блочного алгоритму шифрування з застосуванням штучної нейронної мережі. Кожен блок шифрується з використанням свого ключа, залежного від попереднього тексту і шифротекста. Даний підхід дає можливість вибору закритого ключа шифрування, який виникає за коротким кодом, який супроводжує повідомлення.

В роботі [6] нейромережевий алгоритм шифрування базується на пошуку спотвореного коду, який може розпізнати або відновити використовувану мережу з заданими характеристиками. Запропонований алгоритм належить до блокових шифрів, тому що ключем шифрування і дешифрування є сама нейромережа, а саме фіксованим числом вхідних елементів і внутрішнім поданням даних.

В роботі [7] запропоновано модифікації блокового шифру AES використовуючи нелінійну нейронну мережу. Нейронної мережа виконує процеси шифрування і дешифрування з використанням симетричного ключового шифру. Ключем, що використовується в процесах шифрування і дешифрування, є початкові ваги нейронної мережі, а потім тренується до кінцевої ваги за допомогою швидкого і дешевого алгоритму, такого як алгоритм Левенберга – Марквардта.

Висновки

Розглянуті блокові шифри, реалізовані з використанням штучних нейронних мереж, здатні з необхідною ефективністю вирішувати завдання класичної криптографії. У плані стійкості алгоритми на базі штучних нейронних мереж проявляють себе як більш надійні, так як частина атак на класичні алгоритми для них неприйнятна. У той же час вони не позбавлені недоліків: велика кількість моделей (важко вибрати конкретну модель, налаштувати її параметри), необхідність попередньої обробки даних, суттєві витрати за часом на навчання мережі.

REFERENCES

1. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.
2. Червяков Н.И. Применение искусственных нейронных сетей и систем остаточных классов в криптографии / Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриенко И.Н., Лавриенко А.В. – Москва: Физматлит, 2012. – 270 с.
3. Васюра А.С. (2008), Методи та засоби нейроподібної обробки даних для систем керування / А.С. Васюра, Т.Б. Мартинюк, Л.М. Куперштейн; – Вінниця: УНІВЕРСУМ – Вінниця, – 175 с.
4. Marshalko, “On the security of a neural network-based biometric authentication scheme”, Матем. вопр. криптогр., 5:2 (2014), 87–98.
5. Добрица В.П., Липунов А.А. Нейросетевой шифратор текстов: Известия Юго-Западного государственного университета, 2011, № 5 (38), часть 1, С. 93-97.
6. Евдокимов И. А., Солодовников В. И. Анализ криптостойкости нейросетевого алгоритма симметричного шифрования. — Новые информационные технологии в автоматизированных системах, 2016, № 19, 263–269.
7. Siddeeq, Y.A., Ali, H.M.: AES cryptosystem development using neural networks. International Journal of Computer and Electrical Engineering (IJCEE) 3(2), 309–314 (2011).
8. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.

Татарчук Артем Євгенович — студент, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, Україна

Куперштейн Леонід Михайлович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Tatarchuk Artem — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University

Kupershtein Leonid — PhD, Associate Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia