УДК 004.8+004.056

Л. М. Куперштейн
А. Є. Татарчук

АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ НЕЙРОКРИПТОГРАФІЇ

Вінницький національний технічний університет

Анотація
Розглядається застосування штучних нейронних мереж в криптографії. Наведено приклади використання нейромереж в шифруванні, обміні ключів, хешуванні.
Ключові слова: штучні нейромережі, нейрокриптографія, хешування

Abstract
Application of artificial neural networks in cryptography is considered. Examples of using neural networks in encryption, key exchange, hashing are given.
Keywords: artificial neural networks, neurocryptography, hashing

Вступ

За останні кілька років спостерігається підвищення інтересу до нейронних мереж, які успішно застосовуються в найрізноманітніших областях − бізнесі, медицині, техніці, геології, фізиці. Нейронні мережі увійшли в практику всюди, де потрібно вирішувати завдання прогнозування, класифікації або правління. Обчислювальна потужність нейронних мереж визначається їх паралельною розподіленою структурою і властивою їм здатністю адаптації до певних завдань, до навчання і узагальнення. Ці характеристики дозволяють штучним нейронним мереж вирішувати складні завдання криптографії. Метою роботи є аналіз актуальних проблем, пов'язані з криптографічними методами захисту даних, заснованих на використанні механізмів штучних нейронних мереж.

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. Зрозуміло, нейромережевим технологіям на сьогоднішній час не під силу створити що-небудь, що хоч віддалено нагадує за складністю людський мозок, проте вже дуже багато його функції цілком піддаються моделювання, хоча і в дуже спрощеному варіанті. У тому числі і пряма передача інформації від однієї нейронної мережі іншій в процесі взаємного навчання [2].

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

В криптоаналізі використовується здатність нейронних мереж (НМ) досліджувати простір рішень. Також є можливість створювати нові типи атак на існуючі алгоритми шифрування, засновані на тому, що будь-яка функції може бути представлена нейронною мережею. Зламавши алгоритм, можна знайти рішення, принаймні, теоретично. При цьому використовуються такі властивості нейронних мереж, як взаємне навчання, самонавчання, і стохастична поведінка, а також низька чутливість до шуму, неточностей (спотворення даних, вагових коефіцієнтів, помилки в програмі). Вони дозволяють вирі-

шувати проблеми криптографії з відкритим ключем, розподілу ключів, хешування і генерації псевдовипадкових чисел, візуальної криптографії, стеганографії, шифруванні [2].

Сама модель штучних нейронних мереж добре підходить для побудови хеш-функцій на її основі. Штучний нейрон є базовим блоком при побудові НМ та має n входів, n вагових характеристик по одній на кожен вхід, зміщення, яке подається на вхід функції активації і одне вихідне значення. Таким чином, знаючи вхідний вектор обчислити вихідне значення легко, проте завдання отримання вхідного вектора нейрона за відомим значенням представляється важкою задачею [3]. На підставі цих міркувань можна зробити висновок про те, що штучні нейронні мережі мають властивість односпрямованості. В роботі [4] показано побудову алгоритму хешування з використанням штучних нейронних мереж, яка має властивість однобічності, високої чутливості вихідного значення до вхідних даних і ключа користувача. В роботі [5] запропоновано алгоритм навчання хеш-значення, яке вирішує NP-задачу. В монографії [6] запропоновано метод візуального пошуку на основі хешування.

Також модель штучної нейронної мережі підходить для задач шифрування. Нейронні мережі використовуються для класифікації та апроксимації функцій, виділення завдань, які стійкі до деяких неточностей, для яких є багато доступних даних для навчання, але до яких не можуть бути застосовані жорсткі правила. В статті [7] представлено реалізацію Rijndael-криптосистеми за допомогою НМ. Ця криптосистема має менш складну будову, ніж AES і нелінійна в експлуатації. Нелінійною 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 НМ. Нелінійність необхідна для зменшення ймовірності злому алгоритму. Зменшення ймовірності злому досягається за допомогою нелінійної функції активації. В роботах [8, 9] запропоновано алгоритм машинного навчання, який використовує глибокі нейронні мережі, для вирішення задачі забезпечення конфіденційності інформації на основі шифру AES.

Для обміну ключами між двома абонентами найбільш часто використовується алгоритм Діффі-Хеллмана. Його більш безпечна заміна заснована на синхронізації двох деревовидних машин парності (TPM, tree parity machines). Синхронізація цих машин схожа на синхронізацію двох хаотичних осциляторів в теорії хаотичних зв'язків (chaos communications) [10].

Також, було встановлено, що захищеність звичайних криптографічних систем можна поліпшити, збільшивши довжину ключа. У нейрокриптографії замість ключа збільшується синаптична довжина. Це збільшує складність атаки експоненціально, в той час як витрати абонентів на дешифрування ростуть поліноміально. Таким чином, злом подібної системи є NP-складною задачею [11].

Висновки

Розглянуті криптографічні методи, реалізовані з використанням штучних нейронних мереж, здатні з необхідною ефективністю вирішувати завдання класичної криптографії, такі як забезпечення конфіденційності, цілісності, неможливості відмови від авторства і т.д. Так само штучні нейронні мережі можуть з успіхом застосовуватися для реалізації алгоритмів обміну ключами, що само по собі є однією з найважливіших задач. Теоретичні дослідження доводять ряд переваг, пов'язаних, перш за все, з ускладненням криптоаналізу подібних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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. Dourlens, S., The first definition of the Neuro-Cryptography (AI Neural-Cryptography) applied to DES cryptanalysis by Sebastien Dourlens – 1995, France.

3. A. S. Vasyura, T. B. Martyniuk, and L. M. Kupershtein, Methods and Tools of Neuron-Like Data Processing for Control Systems. A Monograph [in Ukrainian], Universum–Vinnitsa, Vinnitsa (2008).

4. T. Do, A. Doan, N. Cheung, "Learning to hash with binary deep neural network", Proc. Eur. Conf. Comput. Vis., pp. 219-234, 2016.

5. W. Liu, H. Ma, H. Qi, D. Zhao, and Z. Chen, “Deep learning hashing for mobile visual search,” EURASIP J. Image and Video Processing, vol. 2017, pp. 17, 2017.

6. Latha P., Dr. L. Ganesan and Dr. . S. Annadurai, “Face Recognition using Neural Networks”, Signal Processing: An International Journal (SPIJ) Volume (3): Issue (5) pp153-160.

7. W. Liu, H. Ma, H. Qi, D. Zhao, and Z. Chen, “Deep learning hashing for mobile visual search,” EURASIP J. Image and Video Processing, vol. 2017, pp. 17, 2017.

8. Lian, J.S. Sun, Z.Q. Wang. Security Analysis of A Chaos-based Image Encryption Algorithm. Physica A: Statistical and Theoretical Physics, Vol. 351, No. 2-4, 15 June 2005, pp. 645-661

9. Singh, Ajit; Nandal, Aarti (May 2013). "Neural Cryptography for Secret Key Exchange and Encryption with AES" (PDF). International Journal of Advanced Research in Computer Science and Software Engineering. 3 (5): 376–381.

10. E. Hesamifard, H. Takabi, M. Ghasemi. CryptoDL: Towards Deep Learning over Encrypted Data. Annual Computer Security Applications Conference (ACSAC 2016), Los Angeles, California, USA.

11. Shiguo Lian, Jinsheng Sun, Zhiquan Wang. One-way Hash Function Based on Neural Network.

12. Marshalko, “On the security of a neural network-based biometric authentication scheme”, Матем. вопр. криптогр., 5:2 (2014), 87–98

13. 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.

14. 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