ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У КРИПТОГРАФІЇ

Левченко Р. Р., Руженцев В. І.
Харківський національний університет радіоелектроніки, Харків, Україна

В [1] для атак на DES потрібні лише 2^{11} відкритого тексту – шифротексту, щоб навчити нейронну мережу розшифровувати будь-який шифртекст. У той же час, для найбільш відомих атак на DES потрібно більше 2^{40} таких пар, і цей алгоритм є одним з найбільш добре вивчених світовим криптографічним співтовариством протягом 40 років. Використання НМ дозволяє отримати результати, яких ще ніхто не отримував. **Метою доповіді** є розгляд можливості застосування нейронних мереж для атаки на алгоритм шифрування. У якості алгоритму шифрування використовується запропонований алгоритм шифрування, на вхід якого подається повідомлення довжиною 8 бітів. Далі повідомлення роз'єднується на дві рівні частини: ліву та праву. Кожні 4 біти проходять через відповідний S-box, сполучаються і складуються з константним ключем. У кінці виконується циклічний зсув уліво на 5 бітів. Отримуємо 8 бітів на виході. У роботі використовується 3, 5, 7 і 10 раундів шифрування. Для розшифрування зашифроване повідомлення проходить усі операції у зворотному порядку. Для розшифрування повідомлення використовуємо модель багатошарового персептрона: вхідний шар, який має 8 вузлів, прихований із n кількістю нейронів та вихідний із 8 вузлів. Схема зв'язку вузлів наступна: кожен зв'язаний із сусіднім, тобто кожен сингал нейрону першого шару зважується у кожному нейроні прихованого шару, вихідний сигнал яких зважується у кожному нейроні вихідного шару. На вхід БШП подається шифротекст у вигляді 8 бітів. Експерименти показали кореляцію між кількістю нейронів у прихованому шарі БШП та отриманні точного відкритого тексту. Експеримент проводився на виборці 70% від загальної. Тестувалися 4 раунди, які вказали на взаємозв'язок необхідності збільшення кількості нейронів у прихованому шарі та кількості циклів шифрування. Спочатку, іде спад помилок, а потім їх кількість знову зростає. Найкраща кількістю нейронів у прихованому шарі є 96 нейронів із часом навчання у 547,8 секунд ≈9 хвилин. З отриманих результатів видно, що нейронні мережі – це можливе рішення багатьох питань, які ми маємо в області криптографії [2]. Проект демонструє, можливості нейронної мережі на простому алгоритмі шифрування, який недостатньо ефективний для забезпечення безпечного передання інформації.

Список літератури

1. M. M. Alani, "Neuro-cryptanalysis of des," in World Congress on Internet Security (WorldCIS-2012), June 2012, pp. 23–27. DOI: 10.1007/978-3-642-34500-5 75.

2. A Machine Learning Approach for Cryptanalysis Kowsic Jayachandiran Department of Computer Science Golisano College of Computing and Information Sciences Rochester Institute of Technology Rochester, NY 14586