ВИКОРИСТАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У КРИПТОАНАЛІЗІ БЛОЧНОГО СИМЕТРИЧНОГО ШИФРУ AES

Кохан С.А., Руженцев В.І.
Харківський національній університет радіоелектроніки, Харків, Україна

З розвитком технологій машинного навчання, з'являються нові підходи та методи криптоаналізу шифрів. За останні роки набуває популярності метод криптоаналізу який базується на використанні штучних нейронних мереж.

В процесі навчання на вхід нейронної мережі подається шифртекст, а очікуваним виходом є відкритий текст. Після навчання з достатньою кількістю пар відкритих текстів і шифртексту, які зашифровані одним і тим же ключем, нейронна мережа зможе генерувати відкритий текст із зашифрованого тексту, який не був частиною процесу навчання, якщо цей шифртекст зашифрований одні і тим же ключем. Таким чином, результатом даної атаки є функціональний алгоритм еквівалентний початковому дешифруванню за винятком відсутності ключа, використовуваного в процесі шифрування.

У роботі [1] дана атака застосовується до алгоритму блочного шифрування AES з режимами роботи ECB та CBC. В якості нейронних мереж були використані нейронна мережа прямого поширення, а також каскадна нейронна мережа прямого поширення. Дослідження проводилося з різною кількістю біт шифртекстів та відкритих текстів для навчання нейронної мережі, а саме від 2^8 до 2^{13}. При дослідженні нейронної мережі прямого поширення вдалося повністю відновити від 500 до 700 байт відкритого тексту з 2^{17} байт. Кількість біт яка використовувалась при навчанні нейронної мережі не вплинула на кінцевий результат. При використанні каскадної нейронної мережі прямого поширення вдалося повністю відновити від 800 до 5300 байт відкритого тексту з 2^{17} байт. Каскадна нейронна мережа, при навчанні якої використовувалось 2^{13} біт відкритих текстів та шифртекстів показала кращій результат.

Проведений аналіз атаки на шифр AES показав, що для успішної реалізації атаки за допомогою нейронних мереж може знадобитися менша кількість пар відкритих та закритих текстів, ніж для реалізації атаки перебором.

Наведені результати показують, що дуже важливим є вибір топології нейронної мережі, її тип, а також кількість біт яка використовується для її навчання. У зв'язку з цим наступним кроком є дослідження та використання різноманітних типів нейронних мереж для криптоаналізу сучасних шифрів. Отримані результати можуть бути використані як універсальний інструмент аналізу стійкості криптографічних алгоритмів.

Список літератури

1. Xinyi Hu and Yaqun Zhao. Research on Plaintext Restoration of AES Based on Neural Network. Hindawi Security and Communication Networks Volume 2018, Article ID 6868506, 9 pages https://doi.org/10.1155/2018/6868506