АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗНАХОДЖЕННЯ ПРООБРАЗІВ ГЕШ-ФУНКЦІЙ

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

Розвиток обчислювальної техніки вже дійшов тієї стадії, коли є можливість створювати потужні штучні нейронні мережі. Адже на початку заснування теорії про них, вони не набрали популярність через складності з обробкою великих масивів даних.

Нейронні мережі імітують роботу невеликої частини мозку людини. Є набір нейронів поєднаних між собою, які вирішують поставлені задачі. Під час діяльності людини у неї активуються різні частини мозку, так і в нейронних мережах, тобто кожна виконує свої завдання.

Використання нейронних мереж знайшло своє місце у музичних додатках, які за сотнями параметрів рекомендують вам пісні, в комп'ютерних іграх і графічному дизайні, аби зображення на моніторі було на високому рівні при використанні недостатнього потужного обладнання, в мистецтві, де за декількома слова мережа створює зображення, яке захоплює дух.

Метою моєї роботи буде перевірка можливості використання нейронних мереж для успішного знаходження прообразів першого роду популярних геш-функцій. При побудові криптографічно стійких геш-функцій до них висуваються наступні умови: незворотність, висока складність знаходження прообразу, висока складність знаходження другого прообразу та висока складність знаходження колізій. Під другим прообразом мають на увазі, що для заданого повідомлення M має бути обчислювально неможливо підібрати інше повідомлення N, яке має таке ж геш-значення.

Для дослідження функцій буде реалізовано декілька нейронних мереж, адже не можна сказати одразу що є якийсь конкретний тип який нам підійде. Після навчання мережі даними типу «хеш-вхідне повідомлення» спробуємо дегешувати тестовий хеш. Можливо виявиться, що ми можемо отримати лише певні біти, замість цілого тексту.

Геш-функції є основою в криптографічних протоколах, цифрових підписах, відомому протоколі Bitcoin, декартових деревах, фільтрах Блума і цей список можна перелічувати ще довго. Тому ця тема є актуальною, адже має бути впевненість у стійкості та безпеці геш-функції.

Список літератури

1. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. — Введ. 01–04–2015. — К.: Мінекономрозвитку України, 2015.

2. Євсеєв С.П. Йохов О.Ю. Король О.Г. Гешування даних в інформаційних системах: монографія. Вид. ХНЕУ, 2013. – 312 с.