УДК 519.7

О.М. Глазок, к.т.н.
Національний авіаційний університет, Київ

НЕЙРОМЕРЕЖЕВИЙ ПРОТОКОЛ ОБМІНУ КЛЮЧАМИ З ВИКОРИСТАННЯМ РОЗШИРЕНОГО ЗСУВНОГО РЕГІСТРУ

Обмін ключами є однією із проблем сучасної криптографії. В сучасному інформаційному середовищі поширеною задачею є встановлення через відкриті канали зв'язку безпечного віртуального каналу зв'язку двох сторін, які до цього не зустрічалися і не мають надійного секретного каналу для передачі таємної інформації в час узгодження ключів. Для цього сторони мають через небезпечний канал зв'язку узгодити сеансовий ключ, який буде відомий тільки легітимним учасникам обміну. За замовчуванням можна вважати, що інформація, яка передається по відкритим каналам, доступна для прослуховування зловмисникові, який намагатиметься отримати узгоджувані ключі. В даний час для розв'язання цієї задачі широко використовується протокол обміну ключами Діффі-Хеллмана. Нейромережеві протоколи обміну ключами розглядаються як можлива безпечна заміна протоколу Діффі-Хеллмана [1]. Розроблені на даний час нейромережеві протоколи обміну ключами в основному засновані на синхронізації двох деревовидних машин парності – це спеціальний тип багатошарової прямої нейронної мережі [2]. Вона складається з K * N вхідних нейронів, K прихованих нейронів та одного вихідного нейрона, де K і N – параметри конкретної архітектури мережі. Входи в мережу можуть отримувати одне з трьох можливих значень: –1, 0, 1. Вихідне значення кожного прихованого нейрона обчислюється як функція його входів: Вихід деревовидної машин парності є двійковим (може дорівнювати +1 або –1). Також може бути використано бінаризований варіант деревовидної машин парності, що називається «машини парності перестановки» [3], де ваги між вхідними та прихованими нейронами є двійковими значеннями, наприклад 0 або 1; вихідні значення прихованих нейронів також є двійковими.

Метою запропонованого протоколу є створення секретного ключа сеансу, спільного для двох сторін A і B, які спілкуються по незахищеному каналу таким чином, що зловмисник, який слухає їх

переговори, не зміг би відтворити вироблений секрет. Для реалізації протоколу дві сторони повинні зберігати загальний секрет (головний ключ), який використовується в розрахунках при створенні сеансових ключів, але не передається по каналу зв'язку. Важливим елементом схеми є генератор псевдовипадкових чисел (PRNG), який створює групу значень для кожного раунду протоколу. У цій схемі пропонується використовувати PRNG на основі схеми розширеного зсувного регістру. Класичний зсувний регістр побудований на основі послідовно сполучених D-тригерах, кожен з яких може зберігати один із двох бінарних станів (0 або 1). Зворотній зв'язок у такому регістрі реалізований у вигляді набору відводів, які беруть значення з виходів деяких елементів регістру; для отримання величини зворотного зв’язку, що подається на вхід регістру на кожному такті його роботи, ці значення додаються за модулем 2. Розширений зсувний регістр складається з елементів, набір станів яких може відрізнятися від бінарної множини. Для визначення величин зворотного зв’язку додавання за модулем 2 замінюється більш загальною функцією, входи та вихід якої є елементами множини набору станів. Таких функцій може бути одна, використана кілька разів, або декілька різних функцій для кожної окремої ланки зворотного зв’язку. Таким чином, робота модуля зворотного зв’язку у розширеному регістрі залежить від набору відводів і набору застосованих функцій відображення. Класичний зсувний регістр є частковим випадком розширеного.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Singh A., Nandal A. Neural Cryptography for Secret Key Exchange and Encryption with AES // Int. J. of Advanced Research in Computer Science and Software Engineering. – 2013. – Vol. 3, Issue 5. – Pp. 376-381.

2. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Червяков Н.И. и др. – М.: Физматлит, 2012. – 279 с.

3. Reyes O., Zimmermann K. Permutation parity machines for neural cryptography. – Physical Review E. 81 (6): 066117. DOI: 10.1103/ PhysRevE.81.066117.