Загалом Maple має дуже велику кількість команд для побудови різного роду графіків функцій та поверхонь. Вони можуть бути як двомірними, так і тримірними. При побудові можна використовувати декартову, полярну, сферичну та циліндричну системи координат.

Список літератури

1. *Режим доступу* https://bondarenko.dn.ua/maple-issledovanie-funktsij-i-postroenie-grafikov/
2. *Режим доступу* https://studfile.net/preview/4497640/
3. *Режим доступу* https://lib.qrz.ru/node/12500
4. *Режим доступу* http://inel.stu.cn.ua/~asr/forstudent/mapl_u/15.htm
5. *Режим доступу* http://programming-lang.com/ru/comp_soft/dyakonov/0/j477.html

УДК 004.032.26:004.056.55

Грущенко В. Ю., здобувач освіти,
Нескородєва Т. В. к.т.н., доцент,
завідувач кафедри комп'ютерних наук та інформаційних технологій

РОЗПОДІЛ КЛЮЧІВ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Донецький національний університет імені Василя Стуса, м. Вінниця

Управління ключами є складною частиною криптографії. Обмін ключами – це метод криптографії, за допомогою якого відбувається обмін криптографічними ключами між двома сторонами, що дозволяє використовувати криптографічний алгоритм [1].

У схемі обміну ключами Діффі – Геллмана кожна сторона генерує пару відкритого/закритого ключів та поширює відкритий ключ. Після отримання справжньої копії відкритих ключів один одного Аліса та Боб можуть вирахувати загальний секрет в автономному режимі. Загальний секрет може використовуватись, наприклад, як ключ для симетричного шифру [2]. Структуру розподілу ключів наведено на рис. 1.

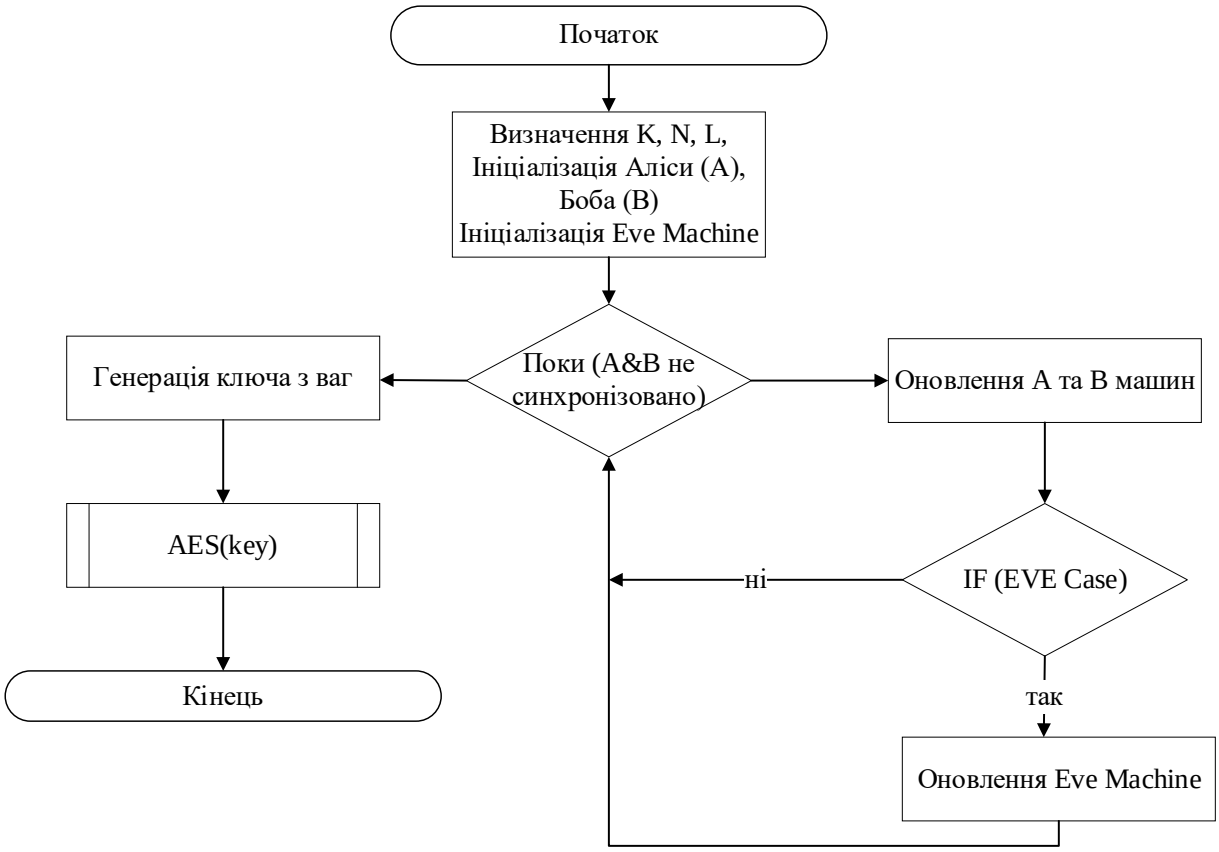

Рис.1 – Структура обміну ключів

Його більш безпечна заміна заснована на синхронізації двох деревовидних машин парності (TPM, tree parity machines) [3].

Вихідний TPM – це багаторівнева мережа прямого поширення, що складається з вхідного, вихідного і одного прихованого рівнів. Вхідний шар складається з N×K двійкові значення, і учасники визначають випадкові (загальні) значення для кожного раунду. Прихований шар складається з незалежних значень, і кожне значення пов'язано N вхідними значеннями [1,4]. Як правило, кількість прихованих блоків фіксовано – з урахуванням безпеки та ефективності. Кожна прихована одиниця обчислюється з використанням N вхідних значень і значень ваги, де значення ваги мають цілочисельні значення – L та L. Індекс i=1,…,K позначає і-й прихований блок, а індекс j=1,2…,N позначає j-е вхідне значення. I- й блок прихований розраховується як добуток відповідних вхідних і вагових значень наступним чином [5]:

$$\sigma_i = sgn(h_i) \quad (1)$$

$$h_i = \frac{1}{\sqrt{N}} W_i \cdot X_i = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} w_{i,j} \cdot x_{i,j} \quad (2)$$

де W_i – вектор вагових значень (наприклад, $W_i = [w_{i1}, w_{i2}, \dots, w_{iN}]$]) та X_i вектор вхідних значень (наприклад $X_i = [x_{i1}, x_{i2}, \dots, x_{iN}]$). Крім того, внутрішнє значення h_i називається локальним полем прихованого шару і sgn(·) є знаковою функцією. Якщо локальне поле h_i прихованого шару є 0, прихована одиниця σ_i встановлюється –1. Отже, вихід τ TPM обчислюється добутком прихованих одиниць [1]:

$$\tau = \prod_{i=1}^{K} \sigma_i, \qquad (3)$$

де результат стає двійковим значенням 1 або −1.

На основі заданої структури TPM відправник і одержувач випадковим чином ініціалізують вагові значення, генерують нові випадкові вхідні значення для кожного раунду та обмінюються розрахунковими вихідними значеннями. Потім вони оновлюють власні значення ваги відповідно до правила навчання, коли результати двох сторін мають однакове значення.

Коли сторони погоджуються оновити ваги за даним правилом навчання, оновлюються лише значення ваги, де відповідна прихована одиниця дорівнює вихідному значенню. В іншому випадку сторони пропускають цей раунд без оновлення ваг і переходять до наступного раунду. Ці процедури повторюються до тих пір, поки вагові вектори не будуть повністю синхронізовані, а однакові вагові вектори можна використовувати як спільний секретний ключ. Безпека оцінюється в кожному окремому випадку за участю зловмисника, якого придумали як машину Єви. Машина Eve являє собою ненадійне джерело з повним знанням криптосистеми та з доступом до вихідних вузлів TPM.

Алгоритм полягає у виконанні наступних кроків:

1.Задання випадкових значень вагових коефіцієнтів

2.Виконання наступних кроків до настання синхронізації

2.1 Генерація випадкового вхідного вектору X

2.2 Обчислення значень прихованих нейронів

2.3 Обчислення значень вихідного вектору

2.4 Порівняння виходів двох TPM

У випадку, якщо виходи різні, то відбувається перехід до 2 пункту. Приклад програмної реалізації наведений на рис. 2

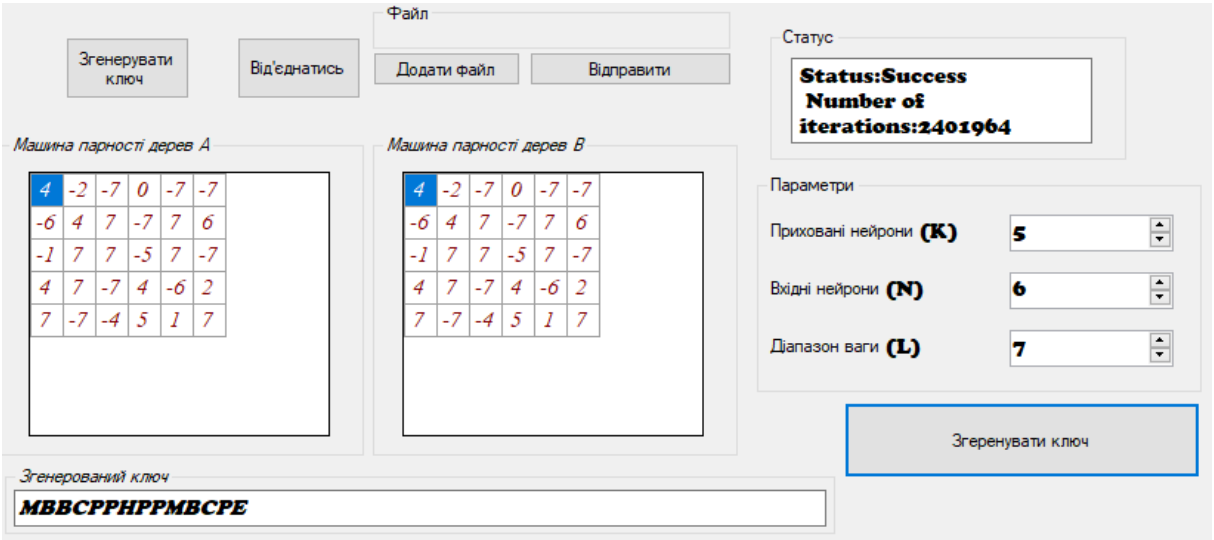

Рис.2 – Програмна реалізація обміну ключів

Висновок. Отже, якщо криптоаналітик повинен перевірити всі можливі варіанти ключів, тобто усі можливі ваги w_{ij}. Якщо є K прихованих нейронів, K×N вхідних нейронів і максимальна вага L, це дає (2L + 1)KN варіантів.

Наприклад, для K = 3, L = 3, N = 100 ≈ $3 \cdot 10^{253}$ різних ключів. На сьогоднішній день така атака неможлива.

Список літератури

1. *Security evaluation of Tree Parity Re-keying Machine implementations utilizing side-channel emissions Jonathan Martínez Padilla, Uwe Meyer-Baese and Simon Foo*
2. *AES Cryptosystem Development Using Neural Networks Siddeeq. Y. Ameen and Ali H. Mahdi International Journal of Computer and Electrical Engineering, Vol. 3, No. 2, April, 2011 1793-8163*
3. *Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems Sooyong Jeong, Cheolhee Park, Dowon Hong, Changho Seo, and Namsu Jho*
4. *Dynamics of neural cryptography Andreas Ruttor, Wolfgang Kinzel, and Ido Kanter Phys. Rev. E 75, 056104 – Published 9 May 2007*
5. *A neural cryptography approach for digital image security using Vigenère cipher and tree parity machine M.A Budiman, Handrizal, William 5 th International Conference on Computing and Applied Informatics (ICCAI 2020)*

УДК 004.931

Гуменний Б.О., здобувач освіти
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій

АВТОМАТИЧНИЙ ДОДАТОК РОЗПІЗНАВАННЯ І ІДЕНТИФІКАЦІЇ ОСІБ ДЛЯ ІОТ

Донецький національний університет імені Василя Стуса, м. Вінниця

Анотація. Показана можливість використовування стандартних скриптів та бібліотек для розроблення автоматичного додатка розпізнавання та ідентифікації осіб для IoT.

Abstract. The possibility is shown, using standard scripts and libraries for development of the automatic application of recognition and identification of persons for IoT.

Розробка і впровадження додатків, таких як розпізнавання обличчя й ідентифікація осіб, нещодавно стала важливою в розумних містах та домах. Як відомо, найбільш використовуваним типом входу для систем безпеки є пароль. Однак завдяки розвитку інформаційних технологій та алгоритмів безпеки багато систем починають використовувати біометричні фактори для завдань розпізнавання й ідентифікації [1,2]. Ці біометричні фактори дозволяють ідентифікувати людей за їх фізіологічними або поведінковими характеристиками. Ці системи мають ряд переваг, наприклад, достатньо присутності людини перед датчиком, і більше не потрібно запам’ятовувати кілька паролів або конфіденційних кодів. У цьому контексті останніми роками було розроблено багато систем розпізнавання на основі різних біометричних факторів, таких як райдужна оболонка ока, відбитки пальців, голос та обличчя.