УДК 004.3

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ НЕЧІТКОЇ СИСТЕМИ

М.П. Карпінський[1], Л.О. Дубчак[2], Н.М. Васильків[2]

[1] Тернопільський національний технічний університет імені Івана Пулюя,
вул. Руська, 56, Тернопіль, 46001, Україна
[2] Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: dlo@tneu.edu.ua

У даній статті розроблено систему вибору методу модулярного експоненціювання, побудовану на основі нечіткої логіки. Дана система дозволяє здійснити оптимальний захист інформації в заданих користувачем умовах.

Ключові слова: модулярне експоненціювання, нечітка логіка, криптозахист, Fuzzy Logic Toolbox

Вступ

Захист інформації є однією з основних задач комерційних чи банківських систем та мереж передачі даних. На даний час в основному застосовуються асиметричні криптосистеми [1]. Базовою операцією в них є модулярне експоненціювання, для здійснення якого можна використати різні методи (наприклад, бінарний, бета-арний, ковзаючого вікна та ін.) [2].

У [5] автори дослідили сучасні алгоритми піднесення до степеня за модулем щодо продуктивності та стійкості до часової атаки. На основі цих результатів можна побудувати систему вибору оптимального методу модулярного експоненціювання при заданих умовах. Найкращим шляхом вирішення цієї задачі є застосування апарату нечіткої логіки.

Теорія нечіткої логіки є узагальненням класичної формальної логіки. Дане поняття було вперше запропоноване американським ученим Лотфі Заде в 1965 р. Основною причиною появи нової теорії стала наявність нечітких і наближених міркувань при описі людиною процесів, систем та об'єктів [3].

Побудова системи вибору методу модулярного експоненціювання на основі нечіткої логіки є актуальною задачею, оскільки дозволяє здійснювати захист інформації без глибоких спеціальних знань у цій галузі.

Основи нечіткої логіки

Характеристикою нечіткої множини виступає функція приналежності. Для опису нечітких множин вводяться поняття нечіткої і лінгвістичної змінних. Нечітка змінна описується набором (N, X, A), де N – це назва змінної, X – універсальна множина (область міркувань), A – нечітка множина на X. Значеннями лінгвістичної змінної можуть бути нечіткі змінні, тобто лінгвістична змінна знаходиться на більш високому рівні, ніж нечітка змінна. Кожна лінгвістична змінна складається з:

- назви;
- множини своїх значень, яка також називається базовою терм-множиною T. Елементами базової терм-множини є назви нечітких змінних;
- універсальної множини X;

- синтаксичного правила G, по якому генеруються нові терми із застосуванням слів природної або формальної мови;
- семантичного правила P, яке кожному значенню лінгвістичної змінної ставить у відповідність нечітку підмножину множини X.

Існує понад десяток типових форм кривих для задання функцій приналежності. Найбільшого поширення набули: трикутна, трапецеїдальна і Гауссова функції приналежності [3].

Трикутна функція приналежності визначається трійкою чисел (a,b,c) і її значення в точці x обчислюється згідно виразу:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a},\ a\le x\le b\\ 1-\dfrac{x-c}{c-b},\ b\le x\le c\\ 0,\text{ в інших випадках}\end{cases} \tag{1}$$

При $(b-a)=(c-b)$ маємо випадок симетричної трикутної функції приналежності, яка може бути однозначно задана двома параметрами з трійки (a,b,c).

Аналогічно для задання трапецеїдальної функції приналежності необхідна четвірка чисел (a,b,c,d):

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a},\ a\le x\le b\\ 1,\ b\le x\le c\\ 1-\dfrac{x-c}{d-c},\ c\le x\le d\\ 0,\text{ в інших випадках}\end{cases} \tag{2}$$

При $(b-a)=(d-c)$ трапецеїдальна функція приналежності набирає симетричного вигляду.

Функція приналежності гауссового типу описується формулою

$$MF(x)=\exp\left[-\left(\frac{x-c}{\sigma}\right)^2\right] \tag{3}$$

і оперує двома параметрами. Параметр c позначає центр нечіткої множини, а параметр σ відповідає за крутизну функції.

Основою для проведення операції нечіткого логічного висновку є база правил, що містить нечіткі висловлення у формі «Якщо-то» і функції приналежності для відповідних лінгвістичних термів. При цьому повинні дотримуватися наступні умови:

- існує хоча б одне правило для кожного лінгвістичного терла вихідної змінної;
- для будь-якого терма вхідної змінної є хоч би одне правило, в якому цей терм використовується як передумова (ліва частина правила).

У загальному випадку механізм логічного висновку включає чотири етапи: введення нечіткості (фазифікація), нечіткий висновок, композиція і приведення до чіткості, або дефазифікація.

Алгоритми нечіткого висновку розрізняються головним чином видом використовуваних правил, логічних операцій і різновидом методу дефазифікації. Розроблені моделі нечіткого висновку Мамдані, Сугено, Ларсена, Цукамото.

Механізм Мамдані − це найбільш поширений спосіб логічного висновку в нечітких системах. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій:

1) Процедура фазифікації: визначаються степені істинності, тобто значення функцій приналежності для лівих частин кожного правила (передумов);

2) Нечіткий висновок;

3) Композиція, або об'єднання отриманих усічених функцій, для чого використовується максимальна композиція нечітких множин;

4) Дефазифікація, або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод.

Класичні нечіткі системи володіють тим недоліком, що для формулювання правил і функцій приналежності необхідно залучати експертів тієї або іншої наочної області, що не завжди удається забезпечити. Адаптивні нечіткі системи вирішують цю проблему. У таких системах підбір параметрів нечіткої системи проводиться в процесі навчання на експериментальних даних. Алгоритми навчання адаптивних нечітких систем відносно трудомісткі і складні в порівнянні з алгоритмами навчання нейронних мереж, і, як правило, складаються з двох стадій: генерації лінгвістичних правил; коректування функцій приналежності. Перше завдання відноситься до задання перераховного типу, друга – до оптимізації в безперервних просторах. При цьому виникає певне протиріччя: для генерації нечітких правил необхідні функції приналежності, а для проведення нечіткого висновку – правила. Крім того, при автоматичній генерації нечітких правил необхідно забезпечити їх повноту і непротирічність [3].

Побудова нечіткої системи вибору методу модулярного експоненціювання

Комп'ютерна система – один із найвразливіших компонентів сучасної фінансово-банківської системи, яка потребує захисту. Будь-яка мережа банківської установи, підприємства чи корпорації може бути захищена від активних атак зловмисників, які можна виявити в процесі експлуатації, завдяки відомим заходам політики безпеки [1]. Проте, існує також можливість виникнення пасивних атак (атака часового аналізу чи аналізу енергоспоживання), які можуть здійснюватись віддалено і тому їх важко виявити.

Усі атаки спеціального виду є досить простими у застосуванні, а їх проведення важко помітити у мережі [4].

Сучасні захищені мережі для здійснення шифрування пакетів інформації та цифрового підпису використовують, як правило, асиметричні криптоалгоритми, основною операцією в яких є модулярне експоненціювання. Вибір оптимального методу піднесення до степеня за модулем забезпечує найвищу швидкодію та стійкість всієї системи.

Для побудови системи вибору методу модулярного експоненціювання необхідно врахувати швидкість виконання алгоритмів кожного з досліджуваних методів (*performance*), стійкість кожного з них до часового аналізу (*resistance*) та довжину ключа (*key*), який використовується для шифрування інформації з застосуванням даних методів.

Засіб *Fuzzy Logic Toolbox* середовища *MathWorks* MATLAB 7.7.0 (R2008b) дозволяє побудувати запропоновану нечітку систему. Першим кроком є задання функцій приналежності для кожної змінної. В якості параметрів задання використано значення швидкодії, стійкості та довжини ключа, поданих у [5]. Для побудови функцій приналежності застосовано трикутну, трапецевидну та дзвоноподібну (як різновид трапецевидної) форми, задані формулами (1) та (2).

Функції приналежності для змінних *performance*, *resistance* та *key* зображено на рис. 1, рис. 2 та рис. 3, відповідно.

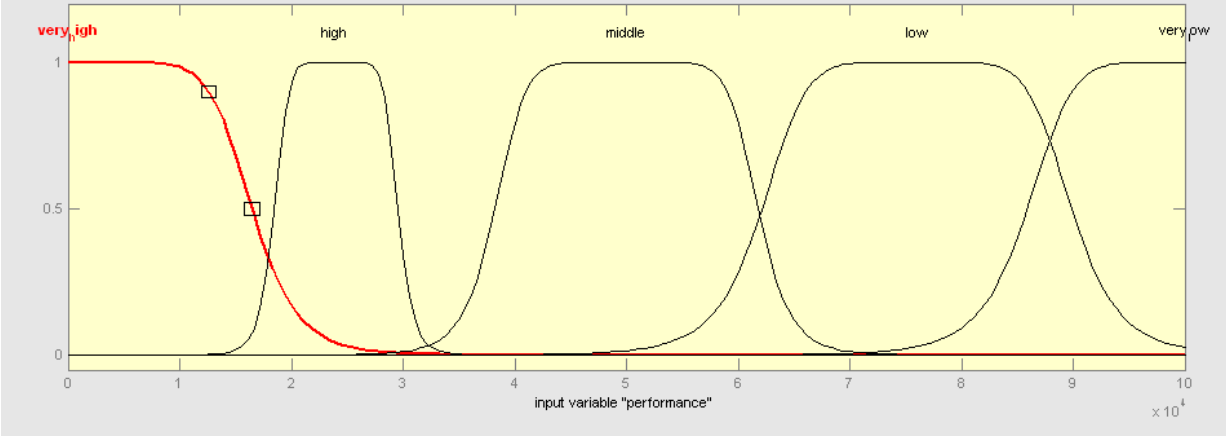

Рис. 1. Функції приналежності змінної *performance*

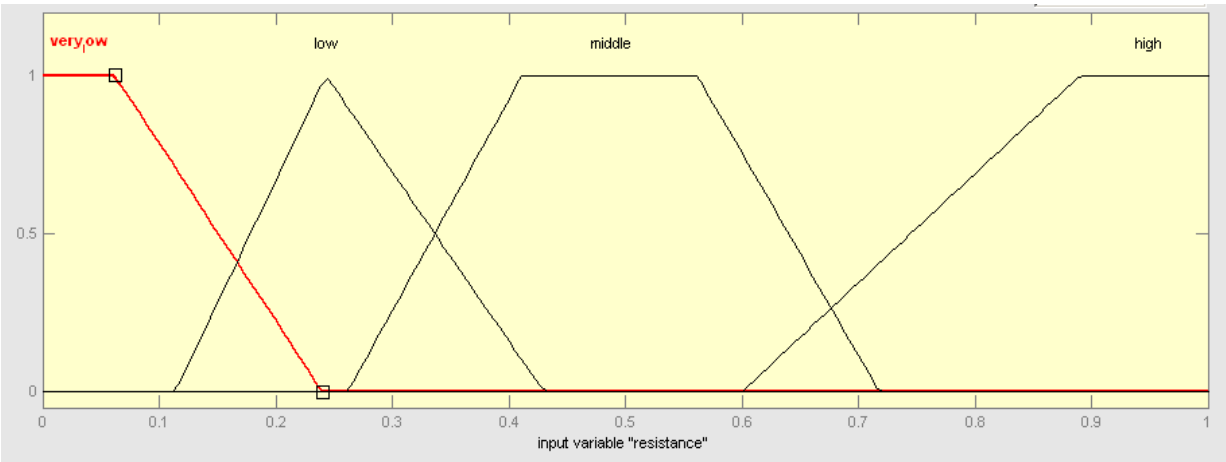

Рис. 2. Функції приналежності змінної *resistance*

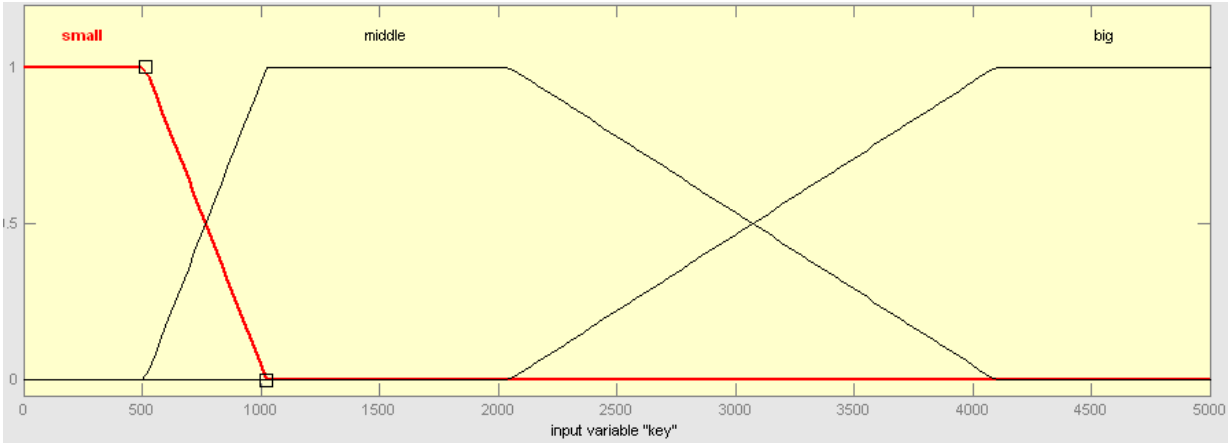

Рис. 3. Функції приналежності змінної *key*

Для вибору методу модулярного експоненціювання застосовано трикутну форму функції приналежності, задану на відрізку [0,1] для зручності сприйняття (рис. 4).

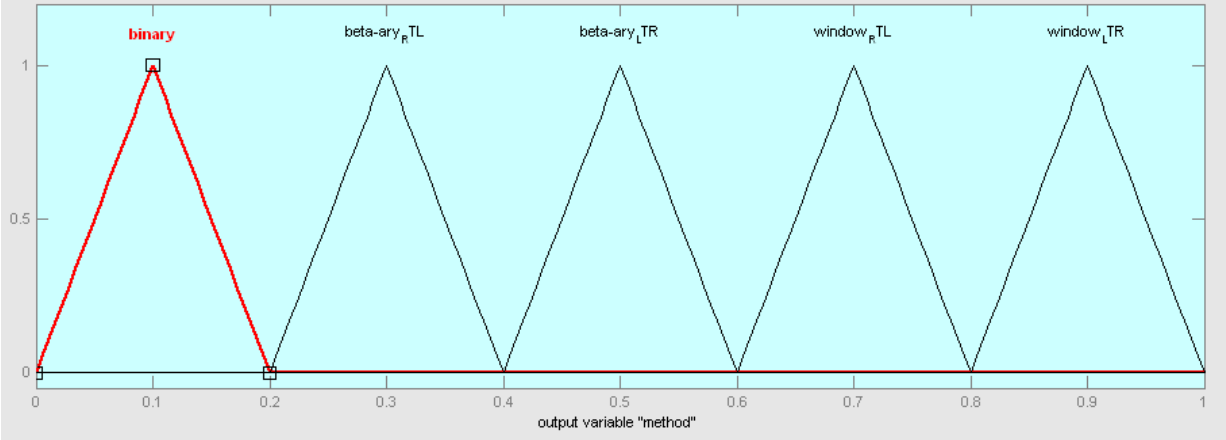

Рис. 4. Функції приналежності вихідної змінної *method*

Система правил складається з 86 нечітких правил типу:

- **IF** (performance is very_high) and (resistance is low) and (key is small) **THEN** (method is beta-ary_RTL)
- **IF** (performance is very_high) and (resistance is very_low) and (key is middle) **THEN** (method is window_LTR)
- **IF** (performance is very_high) and (resistance is high) and (key is small) **THEN** (method is beta-ary_LTR)
- **IF** (performance is high) and (resistance is very_low) and (key is middle) **THEN** (method is binary)
- **IF** (performance is high) and (resistance is middle) and (key is small) **THEN** (method is window_LTR)
- **IF** (performance is middle) and (resistance is low) and (key is small) **THEN** (method is beta-ary_RTL)
- **IF** (performance is middle) and (resistance is high) and (key is small) **THEN** (method is beta-ary_LTR)
- **IF** (performance is low) and (resistance is middle) and (key is small) **THEN** (method is window_LTR)
- **IF** (performance is very_low) and (resistance is very_low) and (key is small) **THEN** (method is binary)
- **IF** (performance is very_low) and (resistance is high) and (key is big) **THEN** (method is beta-ary_LTR)
- **IF** (resistance is middle) and (key is small) **THEN** (method is window_LTR)
- **IF** (resistance is high) and (key is small) **THEN** (method is beta-ary_LTR)
- **IF** (performance is high) and (key is small) **THEN** (method is beta-ary_LTR)
- **IF** (performance is low) and (key is big) **THEN** (method is binary)
- **IF** (performance is very_low) and (key is small) **THEN** (method is window_RTL)

Нечіткий висновок варто вибрати типу Мамдані. Дефазифікація – типу центроїда.

В результаті отримана нечітка система вибору методу модулярного експоненціювання, яка може бути представлена поверхнею значень (рис. 5):

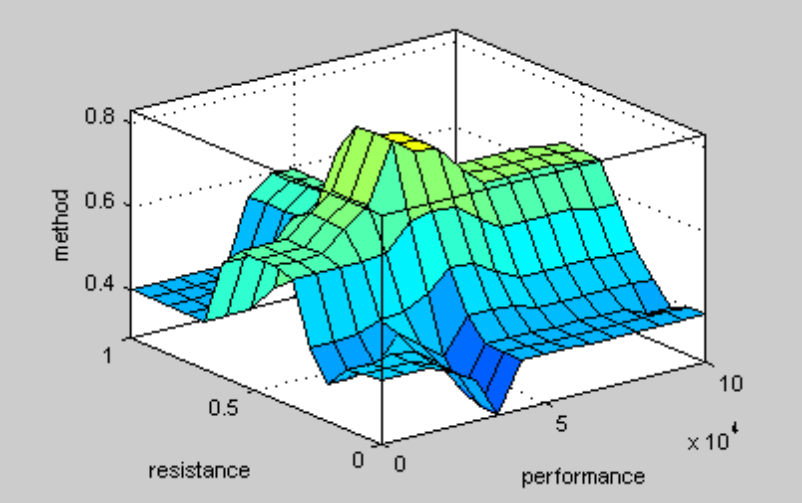

Рис. 5. Поверхня значень нечіткої системи

В результаті проведених досліджень виявлено, що система правил працює вірно. Тобто розроблена нечітка система здатна оптимально вибрати метод піднесення до степеня за модулем, який є найкращим відносно заданих значень довжини ключа, швидкодії та стійкості.

Висновки

В результаті проведених досліджень розроблено нечітку систему вибору методу модулярного експоненціювання, яка дозволяє побудувати захист інформації від часового аналізу, враховуючи необхідний рівень стійкості та продуктивності криптоалгоритмів. Дана система дозволяє будь-якому користувачу забезпечити необхідний рівень захисту його інформації

Подальші дослідження можна проводити за допомогою середовища *MathWorks* Simulink із застосуванням описаної нечіткої системи, що дозволить побудувати апаратний засіб захисту інформації в комп'ютерній мережі.

Список літератури

1. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації: Навчальний посібник. – К.: Вища школа, 2000. – 460 с.
2. Ємець В.,Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. – 144 с.
3. Панкевич О.Д., Штовба С.Д. Діагностування тріщин будівельних конструкцій за допомогою нечітких баз знань. Монографія. – Вінниця: УНІВЕРСУМ-Вінниця, 2005. – 108 с.
4. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними. – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.
5. Карпінський М.П., Васильцов І.В., Дубчак Л.О. Оцінка ризику витоку конфіденційної інформації внаслідок часового аналізу алгоритмів модулярного експоненціювання // Вісник ТДТУ. – 2006. – №4. – С.135-144.

М.П. Карпинский, Л.О. Дубчак, Н.М. Василькив
ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ НЕЧЁТКОЙ СИСТЕМЫ

В данной статье разработано систему выбора метода модулярного экспоненцирования, построенную на основе нечёткой логики. Данная система позволяет осуществить оптимальную защиту информации в заданных пользователем условиях.

Ключевые слова: модулярне экспоненцирование, нечёткая логика, криптозащита, Fuzzy Logic Toolbox

M. Karpinsky, L. Dubchak, N. Vasylkiv
INFORMATION PROTECTION BASED ON FUZZY SYSTEM

This article developed a system of choosing of modular exponentiation method, built on the basis of fuzzy logic. This system allows for optimum protection of information in user-defined conditions.

Keywords: modular exponentiation, fuzzy logic, encryption, Fuzzy Logic Toolbox