УДК 004.3

БАЗА ПРАВИЛ НЕЧІТКОЇ СИСТЕМИ ВИБОРУ МЕТОДУ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ

Дубчак Л.О.
Тернопільський національний економічний університет, аспірант

I. Постановка проблеми

Для сучасних розподілених комп'ютерних мереж, побудованих за схемою Клієнт-Сервер, найнебезпечнішою залишається атака часового аналізу [1].

Захист інформації при передачі пакетів даних здійснюється, в основному, за рахунок застосування асиметричних криптоалгоритмів типу RSA, основною операцією в яких є модулярне експоненціювання. Вибір оптимального методу модулярного експоненціювання відносно поточних умов та можливостей системи захисту інформації є актуальною задачею.

II. Мета роботи

Метою дослідження є розробка бази правил для побудови нечіткої системи вибору методу модулярного експоненціювання, стійкого до часового аналізу.

III. База правил для побудови нечіткої системи

Схема нечіткої системи вибору методу модулярного експоненціювання зображена на рисунку 1. В ній враховується необхідний рівень продуктивності та стійкості до часового аналізу, а також затрати пам’яті сервера, який здійснює передачу захищеної інформації.

Рисунок 1 – Нечітка система вибору методу модулярного експоненціювання

В загальному нечіткий висновок досліджуваної системи вибору будується за принципом Мамдіні [2]. Якщо продуктивність та стійкість до часового аналізу задані нечіткими множинами «висока», «середня» та «низька», а затрати пам’яті – «малі», «середні» та «великі», то база правил складається з 74 правил типу «if-then». Нечіткий висновок досліджуваної система вибору методу модулярного експоненціювання може моделюватися засобами Fuzzy Logic Toolbox середовища MATLAB (рисунок 2).

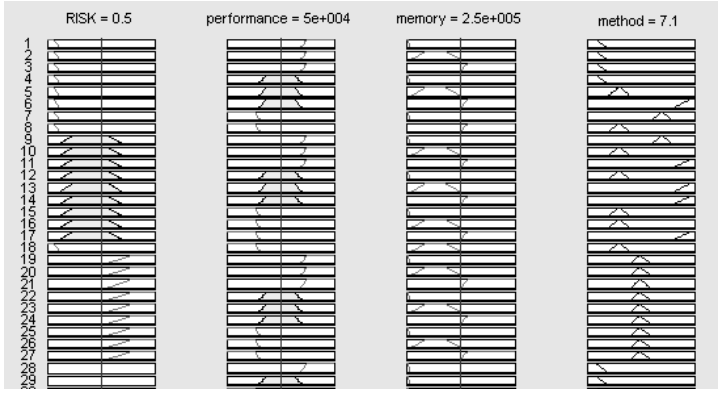

Рисунок 2 – Нечіткий висновок системи вибору методу модулярного експоненціювання

Висновок

У роботі розроблено і досліджено базу правил нечіткої системи вибору методу модулярного експоненціювання.

Список використаних джерел

1. Cathalo J., Koeune F., Quisquater J.-J. A New Type of Timing Attack: Application to GPS.// CHES’2003. - P. 291-303.
2. С.Д.Штовба "Введение в теорию нечетких множеств и нечеткую логику» http://www.matlab.ru/fuzzylogic/book1/index.asp