Бєлозьоров Є.В.

ТЕОРЕТИЧНИЙ ПІДХІД ДО АНАЛІЗУ МОНТАЖУ МЕДІА-СИГНАЛУ, ЩО ЗАСНОВАНИЙ НА ПОРУШЕННІ ПЕРІОДИЧНОСТІ ПРИ КОДУВАННІ

Запропоновано теоретичний підхід, заснований на особливостях теорії кодування медіа-сигналу, що дозволяє аналізувати медіа-сигнал на основі його поділу на окремі блоки, пов'язані з кодуванням сигналу.

Belozerov E.V.

THE THEORETICAL APPROACH TO THE ANALYSIS OF MOUNTING MEDIA SIGNAL BASED ON A VIOLATION OFTHE PERIODICITY IN THE CODING

A theoretical approach based on features of the theory encoded media signal that allows to analyze the media signal based on its division into separate blocks associated with thecoded signal.

УДК 004.942

Дубчак Л.О., Тимошенко Л.М., Яремчук Т.О.

Тернопільський національний економічний університет, Тернопіль

СПОСІБ ВИБОРУ МЕТОДУ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ ДЛЯ ПОБУДОВИ ОПТИМАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Запропоновано систему вибору методу модулярного експоненціювання, який використовується в асиметричних криптосистемах, на основі апарату нечіткої логіки. Такий підхід дозволяє вибрати метод піднесення до степеня за модулем залежно від необхідних параметрів продуктивності та стійкості системи захисту інформації.

Ключові слова: криптосистема, алгоритм модулярного експоненціювання, продуктивність, стійкість, нечітка логіка

Вступ

Захист інформації є зараз дуже актуальною задачею, особливо для соціально-економічних систем. В основному на даний час застосовуються асиметричні криптосистеми, основною операцією яких є піднесення до степеня за модулем (модулярне експоненціювання). Існує багато методів модулярного експоненціювання і всі вони мають різну швидкодію (продуктивність) та стійкість до атак. Актуальною є задача вибору методу піднесення до степеня за модулем у випадку необхідного рівня продуктивності чи стійкості системи захисту інформації.

Практичний досвід розробки систем нечіткого логічного висновку показує, що терміни та вартість їх проектування значно нижчі, ніж при застосуванні традиційного математичного аппарату. Крім цього, забезпечується необхідний рівень працездатності та прозорості моделей.

В даній статті пропонується застосування апарату нечіткої логіки для побудови системи вибору методу модулярного експоненціювання.

Основна частина

В асиметричних криптосистемах, зокрема RSA та Ель-Гамаля, основною операцією, що використовується в процесі шифрування та розшифрування, є модулярне експоненціювання (функція дискретного піднесення до степеня):

$$f(n) = x^n \pmod m, \qquad (1)$$

де n – ціле число ($1 \le n \le m-1$),
m – велике просте число,
x – ціле число ($1 \le x \le m$).

Оскільки для забезпечення стійкості двоключових систем необхідно використовувати досить великі значення x та p, то виникла потреба у використанні спеціальних методів для спрощення і прискорення процесу обчислення цієї функції. На даний час найчастіше вживаними є методи: бінарний і β-арний методи, метод ковзаючого вікна, а також методи з фіксованим показником, з фіксованою основою та з використанням особливостей модулів. Їх опис подано у [1].

Очевидно, що використовувана криптосистема, яка базується на такій операції, повинна задовольняти певні умови, зокрема, мати високу швидкодію та захищеність до атак зловмисників. Перша проблема вирішується вибором оптимального методу обчислення результату піднесення числа до степеня за модулем. Друга проблема набагато серйозніша і вимагає гарантованого забезпечення стійкості цього методу до атак спеціального виду.

Для дослідження стійкості алгоритмів, описаних вище, необхідно встановити залежність часу виконання відповідного алгоритму від ваги Хемінга [2].

Крім того, результати проведеного у [3] аналізу графіків залежності часу виконання алгоритмів модулярного експоненціювання показують, що абсолютно стійким є той алгоритм, час виконання якого є константним, тобто пряма зображення якого паралельна до осі абсцис. Звідси випливає, що стійкішим до часового криптоаналізу атаки є той алгоритм, для якого кут нахилу кривої $T(n, w, w_i)$ часу його виконання наближається до 0°. Як відомо, $\cos 0^0 = 1$. Тому для оцінки нормованої стійкості алгоритму можна використати таке співвідношення [4]:

$$S = \cos\left(arctg \frac{dT_i}{dH(n)} \right). \qquad (2)$$

Аналізуючи час виконання кожного з методів модулярного експоненціювання можна зробити висновок, що найвищу стійкість до часової атаки забезпечує алгоритм β-арного методу “зліва направо” [4].

В табл. 1 наведено оцінки параметрів кожного алгоритму для $w = 4$ та $w_i = 3$.

Аналіз даних табл. 1 показує, що абсолютно стійким до часової атаки є β-арний метод “зліва направо”. Наступним за стійкістю є метод ковзаючого вікна “зліва направо”. Найменшу стійкість до часового аналізу має бінарний метод [4].

При заданих параметрах найшвидшим алгоритмом модулярного експоненціювання є алгоритм β-арного методу “справа наліво”, який виконується за 3956 такти при $n = 512$, а для довжини $n = 4096$ – за 28150 тактів.

Отже, для побудови сучасних ефективних систем захисту інформації на основі асиметричних криптоалгоритмів найкраще застосовувати реалізацію алгоритму β-арного методу “зліва направо” чи “справа наліво”.

Актуальною на даний час є задача побудови системи вибору методу модулярного експоненціювання, в залежності від вимог до продуктивності та стійкості системи в кожному конкретному випадку. Оскільки кожен користувач системи захисту інформації має свої суб’єктивні оцінки продуктивності та стійкості і він необов’язково повинен мати глибокі теоретичні знання з криптографії, то варто застосувати теорію нечіткої логіки, яка є досить дієвою в таких випадках [5].

Практичне застосування теорії нечітких множин передбачає представлення парамет-

рів стану у вигляді лінгвістичних змінних. Формалізація лінгвістичних значень в рамках теорії нечітких множин здійснюється через функції належності. Найбільш розповсюджені методи побудови функцій належностей ґрунтуються на статистичній обробці експертної інформації та на парних порівняннях [5]. Ці методи застосовуються переважно при розробці чистих експертних систем, які використовують лише експертні знання.

Таблиця 1.

Результати досліджень криптографічної стійкості алгоритмів

Алгоритм	Довжина n, біт	Час виконання, такти	Нормована стійкість S
Бінарний метод "зліва направо"	512	11780	0,062
	1024	23550	
	2048	47110	
	4096	94210	
Бінарний метод "справа наліво"	512	11780	0,062
	1024	23560	
	2048	47110	
	4096	94210	
β -арний метод "зліва направо"	512	4724	1
	1024	9204	
	2048	18160	
	4096	36080	
β -арний метод "справа наліво"	512	3956	0,243
	1024	7412	
	2048	14320	
	4096	28150	
Метод ковзаючого вікна "зліва направо"	512	10970	0,430
	1024	22350	
	2048	44570	
	4096	89020	
Метод ковзаючого вікна "справа наліво"	512	12290	0,114
	1024	21560	
	2048	42590	
	4096	84640	

Для здійснення вибору методу модулярного експоненціювання в залежності від заданих користувачем параметрів продуктивності та стійкості, необхідно спочатку вибрати систему вхідних і вихідних параметрів. В даному випадку вхідними параметрами можуть бути продуктивність (performance), стійкість методу експоненціювання до часового аналізу (resistance) та довжина ключа системи захисту (key), а вихідним – один з методів експоненціювання (method). Загальний вигляд нечіткої системи для вибору методу піднесення до степеня за модулем, побудований засобами FuzzyTools середовища MATLAB, зображено на рисунку 1.

Нечітка база знань в даному випадку буде складатися з 86 правил типу "if-then" і передбачає усі випадки перебору значень вхідних параметрів. Наприклад, деякі з цих правил мають наступний вигляд:

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 low) and (key is big) then (method is beta-ary_RTL);

If (performance is high) and (resistance is very_low) and (key is small) then (method is

binary);

If (performance is middle) and (resistance is very_low) and (key is small) then (method is binary);

If (performance is low) and (resistance is very_low) and (key is middle) then (method is window_RTL).

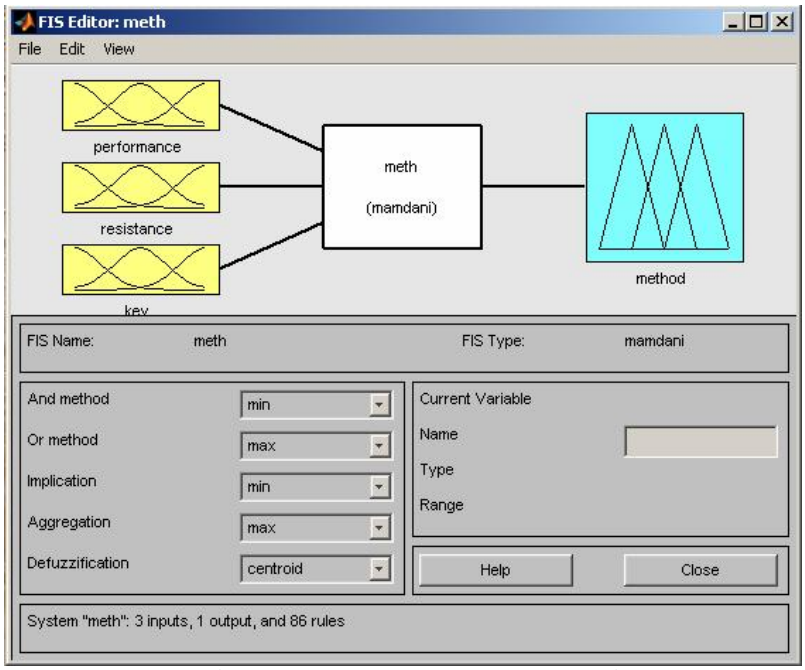

Рис.1. Нечітка система вибору методу експоненціювання

Вигляд поверхні «входи-вихід» побудованої нечіткої моделі буде мати вигляд, зображений на рис.2:

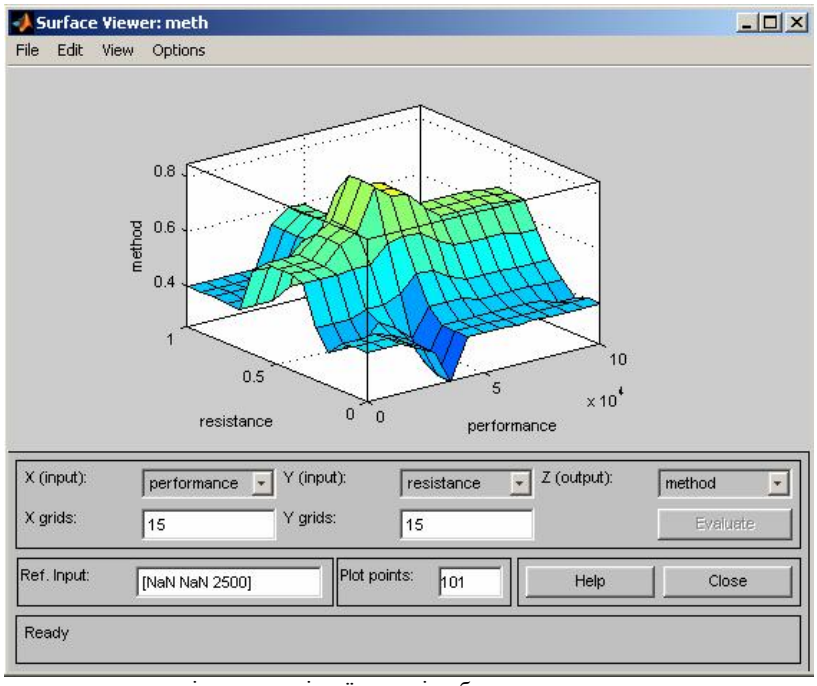

Рис.2. Поверхня «входи -вихід» для нечіткої моделі вибору методу модулярного експоненціювання

Висновки

Запропонований підхід для вибору методу модулярного експоненціювання, базований на апараті нечіткої логіки, дозволяє будь-якому користувачу побудувати оптимальну в кожному окремому випадку систему захисту його інформації. Досить перспективним є розробка апаратного засобу, базованого на розробленій нечіткій системі вибору методу модулярного експоненціювання.

Дана система може використовуватися для побудови оптимальної системи захисту конфіденційної соціальної чи економічної інформації.

Література

1. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. –144 с.

2. Васильцов І.В., Васильків Л.О. Стійкість сучасних алгоритмів модулярного експоненціювання до часового аналізу // Науково-технічний журнал „Захист інформації”, №1, 2005. – Ст. 54-69.

3. Карпінський М., Гізицькі М., Дубчак Л. Secret Key Leakage caused by Hamming-weight Timing Analysis on Modular Exponentiation // Матеріали Міжнародної конференція “Безпека та менеджмент” SAM’06, 26-29

4. Карпінський М.П., Васильцов І.В., Дубчак Л.О. Оцінка ризику витоку конфіденційної інформації внаслідок часового аналізу алгоритмів модулярного експоненціювання – Науковий журнал “Вісник ТДТУ”, №4, 2006, С.135-144.

5 О. Д. Панкевич, С. Д. Штовба. Діагностування тріщин будівельних конструкцій за допомогою нечітких баз знань. Монографія. – Вінниця: УНІВЕРСУМ-Вінниця, 2005. – 108с.

Надійшла до редколегії 14.04.2011

Рецензент: д.т.н., проф.Карпінський М.П., Університет Бєльсько-Бялій, Польша.

Дубчак Л. О.,Тимошенко Л. Н., Яремчук Т. О.

СПОСОБ ВЫБОРА МЕТОДА МОДУЛЯРНОГО ЭКСПОНЕНЦИИРОВАНИЯ ДЛЯ ПОСТРОЕНИЯ ОПТИМАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Предложена система выбора метода модулярного экспоненциирования, который используется в асимметричных криптосистемах, на основе аппарата нечеткой логики. Такой подход позволяет выбрать метод поднесения к степени за модулем в зависимости от необходимых параметров производительности и стойкости системы защиты информации.

Dubchak L.O., Timoshenko L.N., Yaremchuk T.O.

THE CHOICE SYSTEM OF MODULAR EXPONENTIATION METHOD FOR BUILDING OF OPTIMAL CONFIDENT INFORMATION CRYPTOSYSTEM

The choice system of modular exponentiation method, which is used in asymmetric cryptosystems, on the basis of vehicle of fuzzy logic has been proposed. Such approach allows choosing the method of presentation to the degree after the module depending on the necessary parameters of the productivity and resistance of the cryptosystem.

УДК 004.236.321

Павлов І.М., Бірюков В.О.

Військовий інститут телекомунікацій та інформатизації Національного технічного університету України "КПІ", Київ

НЕФОРМАЛЬНИЙ ОПИС ЖИТТЄВОГО ЦИКЛУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

В статті розглянутий порядок аналізу та моделювання життєвого циклу КСЗІ на основі існуючих моделей інформаційних систем. Крім того показані приклади моделей життєвого циклу КСЗІ, які повинні бути проаналізовані розробниками на етапах проектування та розробки КСЗІ.

Ключові слова: аналіз, моделювання, моделі життєвого циклу, проектування.

Життєвим циклом комплексної системи захисту інформації (КСЗІ) називається період існування системи, який пов'язаний з підготовкою до її розробки, розробкою, використанням та удосконаленням під час її роботи, починаючи з того моменту, коли приймається рішення розробити нову систему до того моменту, коли повністю закінчується її повне використання.

Аналіз ряду робіт [1 − 5] показав існуючий опис моделей життєвого циклу інформаційних систем. Для систем захисту інформації чітко не визначені моделі життєвого циклу КСЗІ, хоча в керівних документах та працях прописаний загальний порядок створення КСЗІ [6 − 9]. Тому метою цієї статті є визначення, на основі загальних підходів до життєвих циклів інформаційних систем, опису підходів до аналізу моделей життєвих циклів КСЗІ.

Методологія створення КСЗІ описує процес розробки і супроводження систем у вигляді життєвого циклу, представляючи його як деяку послідовність стадій и процесів, які виконуються. Для кожного етапу визначається склад і послідовність робіт, результати, які необхідно отримати, методи і засоби виконання робіт, а також відповідальність та місце виконавців, тощо. Такий неформальний опис життєвого циклу КСЗІ дозволяє спланувати і організувати процес колективної розробки і забезпечити управління цим процесом [10].

Неформальний опис життєвого циклу КСЗІ базується на дослідженні життєвого циклу, безпосередньо, інформаційної системи,де впроваджується система захисту інформації. Тому при аналізі роботи систем захисту необхідно мати уяву як працює інформаційна система в цілому в процесі усього життєвого циклу. Відповідно розглядаючи життєвий цикл КСЗІ необхідно вишиковувати її життєвий цикл через життєвий цикл інформаційної систе-