Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 004.056 : 004.424.47

МЕТОДИ ТА ЗАСОБИ ФОРМУВАННЯ ВЕКТОРІВ КЕРУВАННЯ ДЛЯ КЕРОВАНИХ ХЕШ-ФУНКЦІЙ

[1]Ю. В. Баришев, аспірант;
[2]О. В. Оводенко, к.т.н., доцент
[1]Вінницький національний технічний університет
[2]Донецький національний технічний університет
[1]yuriy.baryshev@gmail.com, [2]ovoda@i.ua

Останнім часом забезпечення балансу між стійкістю алгоритмів хешування та швидкістю їх виконання стало проблематичним, оскільки з'явилась атака Жукса та похідні від неї загальні атаки, які досягають найбільшої ефективності для розпаралеленого хешування. Причому ці атаки використовують властивість відомих хеш-функцій обробляти дані ітеративно (поблоково), застосовуючи перетворення з однаковими параметрами для кожного блоку даних. Саме тому у зв'язку зі збільшенням кількості загальних атак на хеш-функції необхідно розробити нові підходи до організації багатоканального хешування. До таких підходів належить концепція керованого хешування, реалізація якої вимагає розв'язання низки задач, зокрема задачі формування векторів керування.

У межах наукових досліджень, що проводяться на кафедрі захисту інформації Вінницького національного технічного університету, було запропоновано методи формування вектора керування. Зокрема їх пропонується формувати на основі конкатенації та порозрядного додавання за модулем два проміжних хеш-значень з інших каналів. Для випадку, коли довжина вектора керування n_v у $2a$ раз більша за розрядність каналу n/q (де n – довжи-

на вихідного хеш-значення, q – кількість каналів), пропонується використовувати таке правило:

$$v_i^{(j)} = \left(h_{i-1}^{(j+1)} \| h_{i-1}^{(j+2)} \| \ldots \| h_{i-1}^{(j+a)}\right) \oplus \left(h_{i-1}^{(j+a+1)} \| h_{i-1}^{(j+a+2)} \| \ldots \| h_{i-1}^{(j+2a)}\right)$$

де $v_i^{(j)}$, $h_i^{(j)}$ – вектор керування та проміжне хеш-значення відповідно, які отримані у j-му ($j = \overline{1,q}$) каналі на i-й ($i = \overline{1,l}$) ітерації.

На рис. 1 наведено узагальнену схему формування вектора керування для випадку, коли його довжина не кратна довжині проміжного хеш-значення.

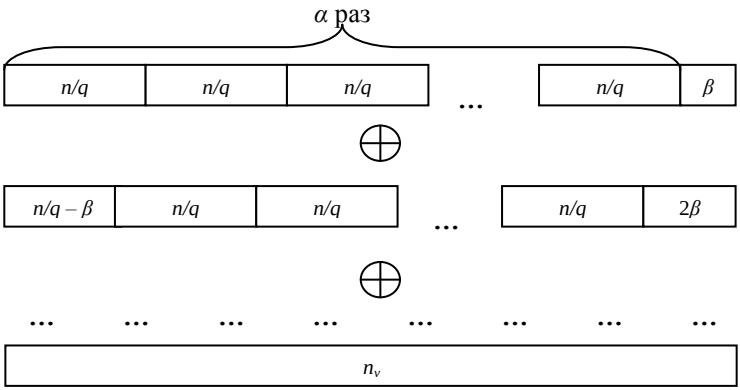

Рисунок 1 – Схема формування вектора керування

Експериментальні дослідження даних методів, виконані на кафедрі радіотехніки та захисту інформації Донецького національного технічного університету, показали, що швидкість програмних реалізацій методів формування векторів керування істотно зростає у випадках, коли довжина вектора керування некратна довжині каналу. Саме тому доцільно використовувати такі функції ущільнення у методах багатоканального керованого хешування, параметри конструкцій яких дозволяють забезпечити цю кратність.