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 ПРОГРАМНІ ЗАСОБИ КЕРОВАНОГО БАГАТОКАНАЛЬНОГО ХЕШУВАННЯ

Ю. В. Баришев, аспірант
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Загальні атаки на хеш-функції стали причиною того, що підходи до хешування, які використовують на кожній ітерації однакові параметри перетворень, виявились нестійкими. Саме тому пропонується використовувати методи керованого хешування, які передбачають зміну параметрів перетворень у функції ущільнення від ітерації до ітерації.

Для реалізації керованого хешування запропонована узагальнена конструкція такого виду:

$$\begin{cases} h_i^{(1)} = f_{v_i^{(1)}}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(k)}, m_i\right) \\ h_i^{(2)} = f_{v_i^{(2)}}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, \ldots, h_{i-1}^{(k+1)}, m_i\right) \\ \ldots \\ h_i^{(q)} = f_{v_i^{(q)}}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, \ldots, h_{i-1}^{(k-1)}, m_i\right) \\ v_i^{(1)} = g\left(h_{i-1}^{(q)}, h_{i-1}^{(q-1)}, \ldots, h_{i-1}^{(q-\phi+1)}\right) \\ v_i^{(2)} = g\left(h_{i-1}^{(1)}, h_{i-1}^{(q)}, h_{i-1}^{(q-1)}, \ldots, h_{i-1}^{(q-\phi+2)}\right) \\ \ldots \\ v_i^{(q)} = g\left(h_{i-1}^{(q-1)}, h_{i-1}^{(q-2)}, \ldots, h_{i-1}^{(q-\phi)}\right) \end{cases}. \qquad (1)$$

де $h_i^{(j)}$ – проміжне хеш-значення, отримане у j-му каналі ($j = \overline{1, q}$) на i-й ітерації ($i = \overline{1, l}$); m_i – i-й блок даних;

$f_{v_i^{(j)}}(\cdot)$ – функція ущільнення, що забезпечує сталу довжину вихідного значення; $v_i^{(j)}$ – вектор керування, який визначає параметри перетворення функції ущільнення $f_{v_i^{(j)}}(\cdot)$ у *j*-му каналі на *i*-й ітерації; $g(\cdot)$ – функція формування вектора керування.

Для реалізації функції ущільнення пропонується використовувати модифіковані шляхом додавання операцій керованого циклічного зсуву та використанням логічного додавання функції, які застосовуються у стандарті хешування SHA-2. Зокрема, пропонується використовувати таку логічну функцію для параметра $k = 4$ конструкції (1):

$$\begin{aligned} h_i^{(j)} = &\left(m_i >>> u_i^{(j)(m1)} \wedge h_{i-1}^{(j)} >>> u_i^{(j)(h1)}\right) \oplus \\ \oplus &\left(m_i >>> u_i^{(j)(m1)} \wedge h_i^{(j+1)} >>> u_i^{(j)(h2)}\right) \oplus \\ \oplus &\left(h_{i-1}^{(j)} >>> u_i^{(j)(h1)} \wedge h_i^{(j+1)} >>> u_i^{(j)(h2)}\right) \oplus \\ \oplus &\left(m_i >>> u_i^{(j)(m2)} \vee h_{i-1}^{(j+2)} >>> u_i^{(j)(h3)}\right) \oplus \\ \oplus &\left(m_i >>> u_i^{(j)(m2)} \vee h_i^{(j+3)} >>> u_i^{(j)(h4)}\right) \oplus \\ \oplus &\left(h_{i-1}^{(j+2)} >>> u_i^{(j)(h3)} \vee h_i^{(j+3)} >>> u_i^{(j)(h4)}\right) \end{aligned} . \qquad (2)$$

Використовуючи функції ущільнення аналогічні (2), було програмно реалізовано методи багатоканального керованого хешування конструкції (1) для різних комбінацій параметрів *q, k,* ϕ цієї конструкції.

За допомогою даних програмних засобів було проведено тестування даних методів хешування за допомогою known-answer tests, а також оцінювання швидкості хешування для вхідних даних різної довжини. Результати цього тестування свідчать про можливість використання запропонованих методів багатоканального керованого хешування на практиці.