Міністерство освіти і науки України

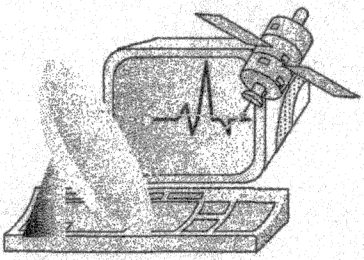
Вінницький національний технічний університет

Вінницька філія ВАТ „Укртелеком"

Інститут кібернетики ім. В.М. Глушкова НАНУ

Вінницьке обласне науково-технічне товариство
радіотехніки, електроніки та зв'язку

Ліга радіоаматорів України



СПРТП-2009

**Матеріали IV Міжнародної
науково-технічної конференції**

СУЧАСНІ ПРОБЛЕМИ РАДІО-ЕЛЕКТРОНІКИ, ТЕЛЕКОМУНІКАЦІЙ ТА ПРИЛАДОБУДУВАННЯ (СПРТП-2009)

*Присвяченої 40-річчю
Факультету радіотехніки та телекомунікацій
Інституту радіотехніки, зв'язку
та приладобудування ВНТУ*

Частина 1

**м. Вінниця, Україна
8 – 10 жовтня 2009 року**

УДК 621.38+621.39+681.2
С 91

Друкується за рішенням Вченої Ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний редактор Н.Г. Курилова

Матеріали статей опубліковані в авторській редакції

С 91 **Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2009).** Матеріали IV міжнародної науково-технічної конференції. м. Вінниця, 8 – 10 жовтня 2009 року. Частина 1. – Вінниця, 2009. – 108 с.

Збірка містить матеріали доповідей IV Міжнародної науково-технічної конференції з сучасних проблем радіоелектроніки, телекомунікацій та приладобудування за такими основними напрямками: теорія кіл, математичне моделювання, захист інформації та програмне забезпечення радіоелектронних, телекомунікаційних та біотехнічних систем; обробка сигналів і зображень в радіоелектронних та телекомунікаційних системах; пристрої радіоелектроніки та засоби телекомунікацій; радіотехнічні, телекомунікаційні та оптоелектронні комплекси та системи; радіоелектронні засоби в біомедичній інженерії; радіовимірювальні пристрої та системи; сучасні аспекти розвитку радіоаматорства

УДК 621.38+621.39+681.2

УДК 003.26

Баришев Ю. (Україна, м.Вінниця)

АЛГОРИТМ ПАРАЛЕЛЬНОГО ХЕШУВАННЯ ДАНИХ

В телекомунікаційних мережах розв'язок задач забезпечення цілісності та автентичності даних часто розв'язують за допомогою хешування. Відомо, що однією з найбільш актуальних задач криптографії, пов'язаних з хешуванням, є пошук найкращого рішення відповідно критерію швидкість/стійкість. Збільшити швидкість хешування дозволяє організація паралельного процесу обчислення хеш-значення. Проте найпростіший випадок паралельного хешування, коли відбувається паралельне обчислення частин хеш-значення та їх конкатенація на завершальній ітерації, виявився криптографічно нестійким до атаки Жукса, яка полягає у пошуку мультиколізій, використовуючи парадокс дня народження, для одного хеш-значення, а потім пошук серед цих наборів колізій такого варіанту, який буде колізією і для іншого хеш-значення, а відтак, цей варіант буде колізією і для результуючого хеш-значення. З цієї причини актуальною задачею є розробка нової математичної моделі або, як її ще прийнято називати, конструкції хешування, яка б забезпечила розпаралелення розрахунків.

Для вирішення поставленої задачі пропонується конструкція хешування, яка передбачає на кожній ітерації паралельне обчислення q частин хеш-значення $h_i^{(1)}, h_i^{(2)}, \ldots, h_i^{(q)}$ в q каналах обчислень з урахуванням всіх частин хеш-значення, отриманих на попередній ітерації в кожному з каналів:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(1)}\right) \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(2)}\right) \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(q)}, m_i, c_i^{(q)}\right) \end{cases}, \quad (1)$$

де $f^{(1)}(\cdot), f^{(2)}(\cdot), \ldots, f^{(q)}(\cdot)$ – функції ущільнення, які мають сталу довжину вихідного значення та обчислюються приблизно за однаковий час;

m_i – i-тий блок інформаційних даних, що хешуються;

$c_i^{(1)}, c_i^{(2)}, \ldots, c_i^{(q)}$ – псевдовипадкові числа, що використовуються з метою протидії атакам з попередньою підготовкою криптоаналітика.

Для конструкції (1) атака Жукса є неможливою, оскільки, знайшовши колізію в одному з каналів обчислення на певній ітерації, зловмисник не може використати її на наступній ітерації для побудови мультиколізії, не перевіривши чи викличе це ж повідомлення колізію в інших $q-1$ каналах з урахуванням їх взаємного впливу.

Практична реалізація конструкції може бути виконана як за допомогою декількох паралельних процесорів, так і на одному процесорі. В останньому випадку розпаралелення розрахунків не відбувається і всі канали обчислень реалізуються послідовно. Якщо функції ущільнення використовують операції множення та піднесення до степеня за модулем, що є характерним для хешування теоретично доведеної стійкості, то конструкція (1) дозволяє скоротити час хешування в q разів при обчисленні n-розрядного хеш-значення за допомогою q n/q-розрядних процесорів, зберігаючи криптографічну стійкість хешування. При реалізації хешування за допомогою одного n/q-розрядного процесора, час хешування з використанням запропонованої конструкції є порівняним з часом хешуванням за допомогою інших конструкцій.