МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

Тези доповідей

Першої міжнародної наукової конференції

ТЕОРІЯ ТА МЕТОДИ ОБРОБКИ СИГНАЛІВ

25-27 травня 2005 року

Київ

УДК 621.391

Перша міжнародна наукова конференція "Теорія та методи обробки сигналів": Тези доповідей. – К.: НАУ, 2005. – 124 с.

Подано матеріали пленарних та секційних доповідей міжнародної наукової конференції "Теорія та методи обробки сигналів". Обговорено основні наукові досягнення. Висвітлено питання методів обробки сигналів.

Для спеціалістів науково-дослідних організацій, викладачів, аспірантів і студентів.

Затверджено до друку вченою радою Інституту електроніки та систем управління Національного авіаційного університету, протокол № 3 від 25 квітня 2005 року.

Наукове видання

Тези доповідей

Першої міжнародної наукової конференції

ТЕОРІЯ ТА МЕТОДИ ОБРОБКИ СИГНАЛІВ

25-27 травня 2005 року

Технічний редактор *А.І. Лавринович*

Підп. до друку 18.05.05 Формат 60x84/16. Папір офс.
Офс. друк. Ум. фарбовідб. 32 Ум. друк. арк. 7,21 Обл.-вид. арк. 7,75
Тираж 175 пр. Замовлення №118-1. Вид. № 9/IV.

Видавництво НАУ
03680, Київ-680, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК №977 від 05.07.2002

СЕКЦІЯ 4. КОДУВАННЯ, СТИСК ТА СПЕКТРАЛЬНИЙ АНАЛІЗ СИГНАЛІВ

Лужецький В.А., В. А. Давидюк

ХЕШ-ФУНКЦІЯ НА ОСНОВІ АРИФМЕТИЧНИХ ОПЕРАЦІЙ ЗА МОДУЛЕМ.

Всі відомі односпрямовані Хеш-функції мають єдину загальну структуру, яка основана на процедурі зчеплення блоків. В найпростішому випадку ця структура має вигляд зчеплення блоків за допомогою операції додавання. Результатом такої функції буде блок, довжина якого дорівнює довжині блоку M_i (i=1..N), на які розбивається повідомлення.

Пропонується будувати хеш-функцію на основі найпростішої хеш-функції, але попередньо розширивши блоки повідомлення. Функція розширення забезпечує односпрямованість. Блок повідомлення з k t-розрядних змінних розширюється до (k+1) t-розрядних змінних. Розширення відбувається за допомогою введення додаткової t-розрядної змінної (K). Після реалізації функції розширення (k+1)*t-розрядному значенню хеш-функції буде відповідати k*t-розрядне значення блоку повідомлення.

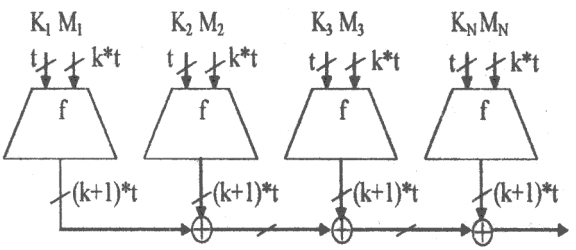

Рис. Структура Хеш-функції з нелінійною функцією розширення.

До тексту повідомлення пропонується дописати довжину повідомлення і розбити його на блоки M_i (i=1..N), де N – останній номер повідомлення. Виходом алгоритму є (k+1)*t-розрядне Хеш-значення.

Після доповнення повідомлення оброблення його відбувається по блочно, тобто блок повідомлення M_i (i=1..N) розширює функція розширення і зчеплює його з попереднім блоком $h_i=f(M_i, h_{i-1})$.

Для функції розширення вибирається змінна К. Для першого блоку змінна К ініціалізується. А для наступного блоку повідомлення потрібно піднести до квадрата константу попереднього блоку і розглянути результат.

Якщо число зі старших t розрядів не дорівнює нулю, то число вибирається як константа, а у випадку рівності нулю беруться t молодших розряди.

На вхід функції розширення поступає константа К і блок повідомлення з k*t біт. Константа і блок повідомлення зберігаються в масиві $M[k+1]=\{K,A_1,A_2, \dots ,A_k\}$. Для збереження результату функції розширення ініціалізується масив з k+1 t-розрядних чисел $M^*[k+1]=\{B_1,B_2, \dots ,B_{k+1}\}$, які дорівнюють нулю.

Реалізація функції розширення відбувається за допомогою операцій множення і додавання за модулем два. Множення і додавання відбувається в першому і другому етапах функції розширення.

Таблиця 1. Результат функції розширення.

$B_1=(KA_1)_L \oplus (((KA_1)_HA_2)_H..A_k)_HK_H \oplus (KA_1)_H \oplus (((KA_1)_LA_2)_L..A_k)_LK_L$
$B_2=(KA_1)_H \oplus ((KA_1)_HA_2)_L \oplus (KA_1)_L \oplus ((KA_1)_LA_2)_H$
$B_3=((KA_1)_HA_2)_H \oplus (((KA_1)_HA_2)_HA_3)_L \oplus ((KA_1)_LA_2)_L \oplus (((KA_1)_LA_2)_LA_3)_H$
. . .
$B_{k+1}=(((KA_1)_HA_2)_H..A_k)_H \oplus (((KA_1)_HA_2)_H..A_k)_HK_L \oplus (((KA_1)_LA_2)_L..A_k)_L \oplus (((KA_1)_LA_2)_L..A_k)_LK_H$

В першому і другому етапах у випадку коли вибраний множник дорівнює нулю, для данного множення береться інша частина результату.