



УКРАЇНА

(19) UA (11) 16332 (13) U
(51) МПК (2006)
G06F 17/00МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС

ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА КОРИСНУ МОДЕЛЬвидається під
відповідальність
власника
патенту

(54) АНАЛІЗАТОР ОБФУСКАЦІЙНИХ АЛГОРИТМІВ

1

(21) u200511063

(22) 22.11.2005

(24) 15.08.2006

(46) 15.08.2006, Бюл. № 8, 2006 р.

(72) Чумаченко Ігор Володимирович, Дергачов
Володимир Андрійович, Малафєєв Євген Євгено-
вич, Шевцов Євгеній Леонідович(73) Чумаченко Ігор Володимирович, Дергачов
Володимир Андрійович, Малафєєв Євген Євгено-
вич, Шевцов Євгеній Леонідович(57) Аналізатор обфускаційних алгоритмів, який
має дві групи інформаційних входів, генератор
імпульсів, двійковий лічильник, елемент І, елемент
НІ, керуючий вхід, вихід наявності даних, шину
результату, формувач адреси, мультиплексор,
демультиплексор, тригери, причому керуючий вхід
з'єднаний з першим входом елемента І, вихід пе-
реповнення двійкового лічильника з'єднаний з ви-
ходом наявності даних та через елемент НІ з дру-
гим входом елемента І, вихід якого з'єднаний з
рахунковим входом двійкового лічильника, вихід
генератора імпульсів з'єднаний з третім входом
елемента І, перша група інформаційних входів
з'єднана з інформаційними входами мультиплек-

2

сора, друга група інформаційних входів з'єднана з
першою групою входів формувача адреси, виходи
двійкового лічильника з'єднані з другою групою
входів формувача адреси та з адресними входами
демультиплексора, виходи формувача адреси
з'єднані з адресними входами мультиплексора,
вихід мультиплексора з'єднаний з інформаційним
входом демультиплексора, виходи якого з'єднані з
входами відповідних тригерів, який **відрізняється**
тим, що містить дешифратор, другий мультиплек-
сор, третю групу інформаційних входів, формувач
фронтів, другий двійковий лічильник, причому ке-
руючий вхід через формувач фронтів з'єднаний з
входами "Скидання" першого двійкового лічильни-
ка та тригерів, виходи тригерів з'єднані з входами
дешифратора, виходи якого з'єднані з інформацій-
ними входами другого мультиплексора, вихід ная-
вності даних з'єднаний з синхронізуючим входом
другого мультиплексора, вихід якого з'єднаний з
рахунковим входом другого двійкового лічильника,
третья група інформаційних входів з'єднана з гру-
пою адресних входів другого мультиплексора, ви-
ходи другого двійкового лічильника з'єднані з ши-
ною результату.

Корисна модель відноситься до обчислюваль-
ної техніки і призначена для аналізу обфускацій-
них властивостей алгоритмічних перетворювачів,
а саме - визначення реалізованості заданої підфу-
нкції при відповідних перетвореннях вхідних опе-
рандів, та підрахунок кількості реалізацій.

Відомий пристрій для логічної обробки інфор-
мації, що містить вхідні шини коефіцієнтів рівнян-
ня, вхідну шину правої частини рівняння, шина
результату, двійковий лічильник, групи з першою
по n-ну елементів І, операційний пристрій, блок
порівняння, тригер, два елементи НІ, два інди-
катори, генератор імпульсів, два елементи І, сумато-
ри по модулю 2, виходи операційного пристрою,
елементи РІВНОЗНАЧНОСТІ [а.с. СРСР
№1262519, кл. G06F 15/20, 1985р.]

Недоліком відомого пристрою є обмежені фун-
кціональні можливості.

Найбільш близьким по технічній суті й резуль-
тату, що досягається є аналізатор алгоритмічних
перетворювачів [Патент України №44172, G06F
17/00. Аналізатор алгоритмічних перетворювачів /
І.В. Чумаченко, Н.В. Доценко, Д.М. Бугас, О.В. Ка-
с'ян, С.Ю. Мелешенко, А.Є. Горобець. -
№2001064097; Заявл. 14.06.2001; Опубл.
15.10.2003, Бюл. №10.], що містить дві групи інфо-
рмаційних входів, генератор імпульсів, двійковий
лічильник, елемент І, елемент НІ, керуючий вхід,
вихід наявності даних, шину результату, формувач
адреси, мультиплексор, демультиплексор, триге-
ри, причому керуючий вхід з'єднаний з першим
входом елемента І, вихід переповнення двійкового
лічильника з'єднаний з виходом наявності даних
та через елемент НІ з другим входом елемента І,
вихід якого з'єднаний з рахунковим входом двійко-
вого лічильника, вихід генератора імпульсів з'єд-

(13) U

(11) 16332

(19) UA

ний з третім входом елемента І, перша група інформаційних входів з'єднана з інформаційними входами мультиплексора, друга група інформаційних входів з'єднана з першою групою входів формувача адреси, виходи двійкового лічильника з'єднані з другою групою входів формувача адреси та з адресними входами демультимплексора, виходи формувача адреси з'єднані з адресними входами мультиплексора, вихід мультиплексора з'єднаний з інформаційним входом демультимплексора, виходи якого з'єднані з входами відповідних тригерів.

Недоліком відомого пристрою є обмежені функціональні можливості, бо він не дозволяє аналізувати обфускаційні властивості алгоритмічних перетворювачів.

В основу корисної моделі поставлено задачу вдосконалити аналізатор алгоритмічних перетворювачів шляхом уведення нового складу елементів, та нової організації взаємозв'язків між ними, забезпечити ширші функціональні можливості при використанні корисної моделі, а саме можливість аналізу обфускаційних властивостей алгоритмічних перетворювачів, та визначення реалізованості заданої підфункції при відповідних перетвореннях вхідних операндів і підрахунок кількості реалізацій.

Поставлене завдання вирішується тим, що аналізатор обфускаційних алгоритмів, який має дві групи інформаційних входів, генератор імпульсів, двійковий лічильник, елемент І, елемент ІІ, керуючий вхід, вихід наявності даних, шину результату, формувач адреси, мультиплексор, демультимплексор, тригери, причому керуючий вхід з'єднаний з першим входом елемента І, вихід переповнення двійкового лічильника з'єднаний з виходом наявності даних та через елемент ІІ з другим входом елемента І, вихід якого з'єднаний з рахунковим входом двійкового лічильника, вихід генератора імпульсів з'єднаний з третім входом елемента І, перша група інформаційних входів з'єднана з інформаційними входами мультиплексора, друга група інформаційних входів з'єднана з першою групою входів формувача адреси, виходи двійкового лічильника з'єднані з другою групою входів формувача адреси та з адресними входами демультимплексора, виходи формувача адреси з'єднані з адресними входами мультиплексора, вихід мультиплексора з'єднаний з інформаційним входом демультимплексора, виходи якого з'єднані з входами відповідних тригерів, згідно з корисною моделлю, має у своєму складі дешифратор, другий мультиплексор, третю групу інформаційних входів, формувач фронту, другий двійковий лічильник, причому керуючий вхід через формувач фронту з'єднаний з входами "Скидання" першого двійкового лічильника та тригерів, виходи тригерів з'єднані з входами дешифратора, виходи якого з'єднані з інформаційними входами другого мультиплексора, вихід наявності даних з'єднаний з синхронізуючим входом другого мультиплексора, вихід якого з'єднаний з рахунковим входом другого двійкового лічильника, третя група інформаційних входів з'єднана з групою адресних входів другого мультиплексора, виходи другого двійкового лічильника з'єднані з шиною результату.

На Фіг.1 представлена функціональна схема

аналізатора обфускаційних алгоритмів.

Аналізатор обфускаційних алгоритмів містить дві групи інформаційних входів 1 і 2, формувач адреси 3, двійковий лічильник 4, елемент І 5, керуючий вхід 6, елемент ІІ 7, вихід наявності даних 8, мультиплексор 9, демультимплексор 10, тригери 11, шину результату 12, генератор імпульсів 13, третю групу інформаційних входів 14, формувач фронту 15, дешифратор 16, другий двійковий лічильник 17, другий мультиплексор 18. Керуючий вхід 6 з'єднаний з першим входом елемента І 5, вихід переповнення двійкового лічильника 4 з'єднаний з виходом наявності даних 8 та через елемент №7 з другим входом елемента І 5, вихід якого з'єднаний з рахунковим входом двійкового лічильника 4, вихід генератора імпульсів 13 з'єднаний з третім входом елемента І 5, перша група інформаційних входів 1 з'єднана з інформаційними входами мультиплексора 9, друга група інформаційних входів 2 з'єднана з першою групою входів формувача адреси 3, виходи двійкового лічильника 4 з'єднані з другою групою входів формувача адреси 3 та з адресними входами демультимплексора 10, виходи формувача адреси 3 з'єднані з адресними входами мультиплексора 9, вихід мультиплексора 9 з'єднаний з інформаційним входом демультимплексора 10, виходи якого з'єднані з входами відповідних тригерів 11, керуючий вхід 6 через формувач фронту 15 з'єднаний з входами "Скидання" першого двійкового лічильника 4 та тригерів 11, виходи тригерів 11 з'єднані з входами дешифратора 16, виходи якого з'єднані з інформаційними входами другого мультиплексора 18, вихід наявності даних 8 з'єднаний з синхронізуючим входом другого мультиплексора 18, вихід якого з'єднаний з рахунковим входом другого двійкового лічильника 17, третя група інформаційних входів 14 з'єднана з групою адресних входів другого мультиплексора 18, виходи другого двійкового лічильника 17 з'єднані з шиною результату 12.

Працює аналізатор обфускаційних алгоритмів таким чином.

Пристрій призначений для аналізу обфускаційних властивостей алгоритмічних перетворювачів, а саме - визначення реалізованості заданої підфункції при відповідних перетвореннях вхідних операндів, та підрахунок кількості реалізацій.

При описі роботи пристрою використані наступні позначення:

n - загальна кількість вхідних змінних,

$X = \{x_1, \dots, x_n\}$ - множина вхідних змінних,

$F(x_1, x_2, \dots, x_n)$ - логічна функція, що описує алгоритм роботи алгоритмічного перетворювача.

Перетворенням вхідних операндів називається заміна деяких змінних на значення із множини $H = \{0, 1, x_1, x_2, \dots, x_n\}$. Під час настройки логічна функція перетворюється у підфункцію від меншої кількості змінних. На інформаційні входи 1 (далі на інформаційні входи мультиплексора 9) подаються значення логічної функції на відповідних двійкових наборах. На інформаційні входи 2 подаються фіксовані значення настроювальних сигналів.

На третю групу інформаційних входів 3 подаються значення заданої підфункції.

Після подачі сигналу "1" на керуючий вхід 6 на

