



УКРАЇНА

(19) UA

(11) 59735

(13) A

(51) 7 G06F7/04

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС

ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ  
НА ВИНАХІДВИДАЄТЬСЯ ПІД  
ВІДПОВІДАЛЬНІСТЬ  
ВЛАСНИКА  
ПАТЕНТУ

## (54) СПОСІБ ПОБУДОВИ ВИСОКОНЕЛІНІЙНИХ ЗБАЛАНСОВАНИХ БУЛЕВИХ ФУНКЦІЙ

1

2

(21) 2002119533

(22) 29 11 2002

(24) 15 09 2003

(46) 15 09 2003, Бюл. № 9, 2003 р.

(72) Потій Олександр Володимирович, Ізбенко  
Юрій Анатолійович, Івашкін Олександр Ва-  
сильович, Головашич Серпій Олександрович  
(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ  
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ(57) Спосіб побудови високонелінійних збалансо-  
ваних булевих функцій, який заснований на вико-  
нанні конкатенації булевих функцій, отриманих  
шляхом модифікації бент-функцій, результатом  
якої є криптографічно стійка функція, в якому про-  
цедуру конкатенації двох булевих функцій над  
 $V_{2k+1}$ , де  $k \geq 1$  виконують згідно з виразом  
 $g(x_1, x_2, \dots, x_{2k+1}) = f(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1}) (x_1 \oplus 1)$ ,  
де  $f(x_2, \dots, x_{2k+1})$  - бент-функція над  $V_{2k}$ ,  $h(x_2, \dots, x_{2k+1})$  -  
неконстантна афінна функція над  $V_{2k}$ ,  $g(x_1,$  $x_2, \dots, x_{2k+1})$  - отримана високонелінійна збалансова-  
на булева функція над  $V_{2k+1}$ , а процедуру конкате-  
нації двох булевих функцій над  $V_{2k+1}$ , де  $k \geq 1$ , ви-  
конують згідно з виразом

$$g(x_1, x_2, \dots, x_3, \dots, x_{2k}) = f(x_3, \dots, x_{2k}) \oplus (x_1 \oplus x_2 \oplus 1) \cdot h(x_3, \dots, x_{2k+1})$$

де  $f(x_3, \dots, x_{2k})$  - бент-функція над  $V_{2k-2}$ ,  $h(x_3, \dots, x_{2k})$  -  
неконстантна афінна функція над  $V_{2k-2}$ ,  $g(x_1, x_2, \dots, x_3, \dots, x_{2k})$  - отримана високонелінійна збалансова-  
на булева функція над  $V_{2k}$ , який відрізняється  
тим, що дозволяє будувати високонелінійні зба-  
лансовані булеві функції з низькими часовими  
витратами та високою непередбачуваністю  
вихідних значень функцій завдяки виконанню про-  
цедури конкатенації двох булевих функцій за до-  
помогою нових виразівЗапропонований винахід відноситься до авто-  
матики й обчислювальної техніки і може бути ви-  
користаний, зокрема, у системах криптографічного  
захисту інформаціїВідомий спосіб побудови високонелінійних  
збалансованих булевих функцій (див. B. Preneel,  
R. Govaerts, and J. Vandewalle, "Boolean functions  
satisfying higher order propagation criteria" in Lecture  
Notes in Computer Science 547, Advances in Cry-  
ptology Proc. Eurocrypt'91, 1991, pp. 141-152, Berlin:  
Springer-Verlag), заснований на конкатенації буле-  
вих функцій. Для виконання побудови використо-  
вується булева функція  $f$  над заданим векторним  
простором  $V_n$ . При цьому побудова складається з  
наступних двох етапів: вибору нелінійної функції  $f$ ,  
яка має нульові значення в спектрі Уолша, резуль-  
татом якого є проміжна булева функція, додавання  
потрібної лінійної функції  $h$  над  $V_n$ , результатом  
якого є високонелінійна збалансована булева  
функція, яка має гарні характеристики розповсюд-  
ження.Наведений аналог потребує багато часу для  
побудови криптографічно стійких булевих функційза рахунок необхідності знаходження нелінійних  
функцій з нульовими значеннями в їхньому спектрі  
Уолша та пошуку необхідної лінійної функції  $h$ , яка  
може бути знайдена шляхом повного перебору  
над всіма лінійними функціями над  $V_n$ .Найбільш близьким по сукупності ознак до за-  
пропонованого способу є спосіб побудови високо-  
нелінійних збалансованих булевих функцій (див. J.  
Sebeny, X.-M. Zhang and Y. Zheng, "Nonlinearity and  
Propagation Characteristics of Balanced Boolean  
Functions", Information and Computation, Vol. 119,  
№1, pp. 1-13, 1995), заснований на конкатенації  
булевих функцій. Побудова складається з вико-  
нання конкатенації двох булевих функцій, отрима-  
них шляхом модифікації бент-функції, результатом  
якої є проміжна булева функція, та виконання  
афінних перетворень координат проміжної булевої  
функції, результатом якої є високонелінійна зба-  
лансована булева функція з гарними характери-  
стики розповсюдження. Процедура виконання кон-  
катенації двох булевих функцій над  $V_{2k+1}$ , де  $k \geq 1$ ,  
отриманих шляхом модифікації бейт-функції, опи-  
сується наступним виразом

(13) A

(11) 59735

(19) UA

$$g(x_1, x_2, \dots, x_{2k+1}) = (1 \oplus x_1)f(x_2, \dots, x_{2k+1}) \oplus x_1(1 \oplus f(x_2, \dots, x_{2k+1})) = x_1 \oplus f(x_2, \dots, x_{2k+1}),$$

де

$f(x_2, \dots, x_{2k+1})$  - бент функція над  $V_{2k}$

$g(x_1, x_2, \dots, x_{2k+1})$  - отримана високонелінійна

$$g(x_1, x_2, x_3, \dots, x_{2k}) = (1 \oplus x_1)(1 \oplus x_2)f(x_3, \dots, x_{2k}) \oplus (1 \oplus x_1)x_2(1 \oplus f(x_3, \dots, x_{2k})) \oplus x_1(1 \oplus x_2)(1 \oplus f(x_3, \dots, x_{2k})) \oplus x_1x_2f(x_3, \dots, x_{2k}) = x_1 \oplus x_2 \oplus f(x_3, \dots, x_{2k}),$$

де

$f(x_3, \dots, x_{2k})$  - бент функція над  $V_{2k-2}$ ,

$g(x_1, x_2, x_3, \dots, x_{2k})$  - отримана високонелінійна збалансована булева функція над  $V_{2k}$

Процедура виконання афінних перетворень координат проміжної булевої функції  $g(x)$  описується формулою

$$g^*(x) = g(Ax),$$

де

$g^*(x)$  - функція, обчислена з  $g(x)$  шляхом лінійного перетворення вхідних координат,

$A$  - невідроджена матриця, така що  $\alpha_j A = \beta_j$  з

базисами  $B_1 = \{\alpha_j \mid j=1, \dots, 2k+1\}$ ,

$B_2 = \{\beta_j \mid j=1, \dots, 2k+1\}$  на  $V_{2k+1}$  та  $B_1 = \{\alpha_j \mid j=1, \dots, 2k\}$ ,

$B_2 = \{\beta_j \mid j=1, \dots, 2k\}$  над  $V_{2k}$

Функція, обчислена над на  $V_{2k+1}$ , є збалансованою, має не лінійність  $N_g \geq 2^{2k} - 2^k$  та задовольняє критерію розповсюдження відносно всіх ненульових векторів, окрім  $\gamma \neq (1, 0, \dots, 0)$ . Функція, обчислена над на  $V_{2k}$  є збалансованою, має не лінійність  $N_g \geq 2^{2k-1} - 2^k$  та задовольняє критерію розповсюдження відносно всіх ненульових векторів, окрім трьох векторів  $\gamma_1 = (1, 0, \dots, 0)$ ,  $\gamma_2 = (0, 1, \dots, 0)$ ,

збалансована булева функція над  $V_{2k+1}$

Процедура виконання конкатенації двох булевих функцій над  $V_{2k}$  де  $k \geq 1$ , отриманих шляхом модифікації бент функції, описується наступним виразом

$$\gamma_3 = \gamma_1 \oplus \gamma_2 = (1, 1, \dots, 0)$$

При реалізації технічного рішення, прийнятого за прототип, потрібно багато часу для побудови криптографічно стійких булевих функцій за рахунок необхідності виконання афінних перетворень координат проміжної булевої функції, крім того, вихідні дані функції є лінійно залежними від  $x_1$  над  $V_{2k+1}$  та від  $x_1, x_2$  над  $V_{2k}$ , що істотно знижує передбачуваність цих вихідних даних

В основу винаходу поставлена задача створити спосіб побудови високонелінійних збалансованих булевих функцій, який дозволив би будувати високонелінійні збалансовані булеві функції з низькими часовими витратами та високою непередбачуваністю вихідних значень функцій завдяки виконанню процедури конкатенації двох булевих функцій за допомогою нових виразів

Такий технічний результат може бути отриманий, якщо у способі побудови високонелінійних збалансованих булевих функцій, заснованому на виконанні конкатенації булевих функцій, отриманих шляхом модифікації бент функцій, результатом якої є криптографічно стійка функція, згідно з винаходом, процедуру конкатенації двох булевих функцій над  $V_{2k+1}$ , де  $k \geq 1$ , виконують згідно з виразом

$$g(x_1, x_2, \dots, x_{2k+1}) = x_1 f(x_2, \dots, x_{2k+1}) \oplus (1 \oplus x_1)(f(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1})) = x_1 f(x_2, \dots, x_{2k+1}) \oplus f(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1}) \oplus x_1(x_2, \dots, x_{2k+1}) \oplus x_1 h(x_2, \dots, x_{2k+1}) = f(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1})(x_1 \oplus 1),$$

де

$f(x_2, \dots, x_{2k+1})$  - бент функція над  $V_{2k}$ ,

$h(x_2, \dots, x_{2k+1})$  - неконстантна афінна функція над  $V_{2k}$ ,  $g(x_1, x_2, \dots, x_{2k+1})$  - отримана високонелінійна збалансована булева функція над  $V_{2k+1}$ , а процедуру конкатенації двох булевих функцій над  $V_{2k}$  де  $k \geq 1$ , виконують згідно з виразом

$$g(x_1, x_2, x_3, \dots, x_{2k}) = (x_1 \oplus x_2)f(x_3, \dots, x_{2k}) \oplus (1 \oplus x_1 \oplus x_2)(f(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k})) \oplus hf(x_3, \dots, x_{2k}) = x_1 f(x_3, \dots, x_{2k}) \oplus x_2 f(x_3, \dots, x_{2k}) \oplus f(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k}) \oplus x_1 f(x_3, \dots, x_{2k}) \oplus x_1 h(x_3, \dots, x_{2k}) \oplus x_2 f(x_3, \dots, x_{2k}) \oplus x_1 h(x_3, \dots, x_{2k}) = f(x_3, \dots, x_{2k}) \oplus (x_1 \oplus x_2 \oplus 1)h(x_3, \dots, x_{2k}),$$

де

$f(x_3, \dots, x_{2k})$  - бент функція над  $V_{2k-2}$ ,

$h(x_3, \dots, x_{2k})$  - неконстантна афінна функція над  $V_{2k-2}$ ,  $g(x_1, x_2, x_3, \dots, x_{2k})$  - отримана високонелінійна збалансована булева функція над  $V_{2k}$

Функція  $g$  над  $V_{2k+1}$  є збалансованою функцією, задовольняє критерію розповсюдження відносно всіх ненульових векторів  $\gamma \in V_{2k+1}$  за винятком вектора  $\gamma$ , обумовленого видом обраної афінної

функції, та має не лінійність  $N_g \geq 2^{2k} - 2^k$ . Функція  $g$  над  $V_{2k}$  є збалансованою функцією, задовольняє критерію розповсюдження відносно всіх ненульових векторів  $\gamma \in V_{2k+1}$ , за винятком трьох ненульових векторів  $\gamma_1, \gamma_2, \gamma_3 = \gamma_1 \oplus \gamma_2$  обумовлених видом обраної афінної функції, та має не лінійність  $N_g \geq 2^{2k-1} - 2^k$

Таким чином, виконання процедури конкатенації двох булевих функцій за допомогою запро-

понованих виразів дозволяє скоротити час, потрібний для побудови високонелінійних збалансованих булевих функцій, щонайменше в 2 рази, та підвищити непередбачуваність вихідних значень функцій

Спосіб побудови високонелінійних збалансованих булевих функцій над  $V_{2k+1}$  може бути реалізований таким чином. Виконується побудова бент функції  $f(x_2, \dots, x_{2k+1})$  над  $V_{2k}$  та рахується кількість "0" та "1" в її вихідній послідовності. Далі виконується побудова випадкової не константної афінної функції  $h(x_2, \dots, x_{2k+1})$  над  $V_{2k}$  та рахується кількість "0" та "1" в вихідній послідовності конкатенації функцій  $f \oplus h$ . Якщо кількість "0" та "1" в вихідній послідовності  $f$  дорівнює кількості "0" та "1" в вихідній послідовності  $f \oplus h$ , то функція  $h$  комплементується одиницею  $h = h \oplus 1$ , інакше - не комплементується. Після визначення  $f$  та  $h$  виконується застосування процедури побудови високонелінійних збалансованих булевих функцій над  $V_{2k+1}$  згідно з виразом

$$g(x_1, x_2, \dots, x_{2k+1}) = f(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1})(x_1 \oplus 1)$$

Результатом застосування є функція  $g$  з високими криптографічними показниками стійкості. Над  $V_{2k}$  побудова високонелінійних збалансованих булевих функцій виконується шляхом побудови бент функції  $f(x_3, \dots, x_{2k})$  над  $V_{2k-2}$  з підрахунком кількості "0" та "1" в її вихідній послідовності. Далі виконується побудова випадкової неконстантної афінної функції  $h(x_3, \dots, x_{2k})$  над  $V_{2k-2}$  та рахується кількість "0" та "1" в вихідній послідовності конкатенації функцій  $f \oplus h$ . Якщо кількість "0" та "1" в вихідній послідовності  $f$  дорівнює кількості "0" та "1" в вихідній послідовності  $f \oplus h$ , то функція  $h$  комплементується одиницею  $h = h \oplus 1$ , інакше - не комплементується. Після визначення  $f$  та  $h$  виконується застосування процедури побудови високонелінійних збалансованих булевих функцій над  $V_{2k}$  згідно з виразом

$$g(x_1, x_2, x_3, \dots, x_{2k}) = f(x_3, \dots, x_{2k}) \oplus (x_1 \oplus x_2 \oplus 1)h(x_3, \dots, x_{2k})$$

Результатом застосування є функція  $g$  з високими криптографічними показниками стійкості.