



УКРАЇНА

(19) UA

(11) 60017

(13) A

(51) 7 G06F7/04

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС

ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ  
НА ВІНАХІДВИДАЄТЬСЯ ПІД  
ВІДПОВІДАЛЬНІСТЬ  
ВЛАСНИКА  
ПАТЕНТУ**(54) СПОСІБ ПОБУДОВИ ВИСОКОНЕЛІНІЙНИХ ЗБАЛАНСОВАНИХ БУЛЕВИХ ФУНКЦІЙ З КОНТРОЛЬОВАНИМ АЛГЕБРАІЧНИМ СТЕПЕНЕМ**

1

2

(21) 2003010323

(22) 14 01 2003

(24) 15 09 2003

(46) 15 09 2003, Бюл. № 9, 2003 р.

(72) Потій Олександр Володимирович, Ізбенко  
Юрій Анатолійович, Головашич Сергій Ана-  
толійович(73) ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ  
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ(57) Спосіб побудови високонелінійних збалансованих булевих функцій з контрольованим алгебраїчним степенем, заснований на виконанні конкатенації булевих функцій, отриманих шляхом модифікації бент функцій, результатом якої є криптографічно стійка функція, який відрізняється тим, що процедуру конкатенації трьох булевих функцій над  $V_{2k+1}$ , де  $k \geq 1$ , виконують згідно з виразом

$$g(x_1, x_2, \dots, x_{2k+1}) = x_1(f_1(x_2, \dots, x_{2k+1}) \oplus \\ \oplus f_2(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1})) \oplus$$

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

де  $f_1(x_2, \dots, x_{2k+1})$ ,  $f_2(x_2, \dots, x_{2k+1})$  - бент функції 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 трьох булевих функцій над  $V_{2k}$ , де  $k \geq 1$ , виконують згідно з виразом

$$g(x_1, x_2, \dots, x_{2k}) = x_1(f_1(x_3, \dots, x_{2k}) \oplus \\ \oplus f_2(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k})) \oplus \\ \oplus x_2(f_1(x_3, \dots, x_{2k}) \oplus f_2(x_3, \dots, x_{2k}) \oplus \\ \oplus h(x_3, \dots, x_{2k})) \oplus f_2(x_3, \dots, x_{2k}) \oplus \\ \oplus h(x_3, \dots, x_{2k}),$$

де  $f_1(x_3, \dots, x_{2k})$ ,  $f_2(x_3, \dots, x_{2k})$  - бент функції 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  $V_{2k}$ 

Запропонований винахід відноситься до автоматики й обчислювальної техніки і може бути використаний, зокрема, у системах криптографічного захисту інформації

Відомий 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 Cryptology Proc Eurocrypt'91, 1991, pp. 141-152, Berlin: Springer-Verlag), заснований на конкатенації булевих функцій. Для виконання побудови використовується 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, результатом якого є проміжна булева функція, додавання потрібної лінійної функції  $h$  над  $V_n$ , ре-зультатом якого є високонелінійна збалансована булева функція. Алгебраїчний степінь отриманої функції дорівнює алгебраїчному степеню початкової функції  $f$ .Наведений аналог потребує багато часу для побудови криптографічно стійких булевих функцій за 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 запропонованого способу є спосіб побудови високонелінійних збалансованих булевих функцій (див. J. Seberry, X.-M. Zhang and Y. Zheng, "Nonlinearity and Propagation Characteristics of Balanced Boolean Functions", Information and Computation, Vol. 119, No. 1, pp. 1-13, 1995), заснований на конкатенації

(13) A

(11) 60017

(19) UA

булевих функцій Побудова складається з виконання конкатенації булевих функцій, отриманих шляхом модифікації бент функцій, результатом якої є високонелінійна збалансована булева функція Процедура виконання конкатенації двох булевих функцій над  $V_{2k+1}$ , де  $k \geq 1$ , отриманих шляхом модифікації бент функцій, описується наступним виразом

$$g(x_1, x_2, \dots, x_{2k+1}) = (1 \oplus x_1) f_1(x_2, \dots, x_{2k+1}) \oplus x_1 f_2(x_2, \dots, x_{2k+1}),$$

де  $f_1(x_2, \dots, x_{2k+1})$ ,  $f_2(x_2, \dots, x_{2k+1})$  - бент функції над  $V_{2k}$ ,  $g(x_1, x_2, \dots, x_{2k+1})$  - отримана високонелінійна збалансована булева функція над  $V_{2k+1}$

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

$$g(x, y) = \bigoplus_{i=0}^3 D_{\alpha} (y) f_i(x),$$

де  $f_i(x)$  - бент функції над  $V_{2k-2}$ ,  $y = (y_1, y_2)$ ,  $x = (x_1, \dots, x_{2k-2})$  та  $\alpha$ ,  $\epsilon$  вектором над  $V_2$ , чийе цілочисельне представлення дорівнює  $i$ ,  $g(y, x)$  - отримана високонелінійна збалансована булева функція над  $V_{2k}$

Функція, обчислена над  $V_{2k+1}$  є збалансованою, має нелінійність  $N_g \geq 2^{2k} - 2^k$  та алгебраїчний степінь  $\deg(g) = \max\{\deg(f_i(x))\} + 1$  Функція, обчислена над  $V_{2k}^{2k}$  є збалансованою, має нелінійність  $N_g \geq 2^{2k-1} - 2^k$  та алгебраїчний степінь  $\deg(g) = \max\{\deg(f_i(x))\} + 1$

При реалізації технічного рішення, прийнятого за прототип, потрібно багато часу для побудови криптографічне стійких булевих функцій над  $V_{2k}$  за рахунок необхідності побудови чотирьох бент функцій з необхідними властивостями, крім того, максимальний алгебраїчний степінь  $\deg(g, x)$ , що дорівнює алгебраїчному степеню отриманих функцій  $\deg(g)$ , мають лише ті координати, що знаходяться в найдовшому доданку функцій, представлених в алгебраїчній нормальній формі, решта координат має менший алгебраїчний степінь, що знижує криптографічну стійкість до атаки криптоаналізу методом диференціалів вищих порядків

В основу винаходу поставлена задача створити спосіб побудови високонелінійних збалансованих булевих функцій з контролюємим алгебраїчним степенем, який дозволив би будувати високонелінійні збалансовані булеві функції з низькими часовими витратами та контролюємим алгебраїчним степенем кожної координати завдяки виконанню процедури конкатенації булевих функцій за допомогою нових виразів

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

$$g(x_1, x_2, \dots, x_{2k+1}) = x_1(f_1(x_2, \dots, x_{2k+1}) \oplus f_2(x_2, \dots, x_{2k+1}), \oplus h(x_2, \dots, x_{2k+1}), \oplus f_2(x_2, \dots, x_{2k+1}), \oplus h(x_2, \dots, x_{2k+1})),$$

де  $f_1(x_2, \dots, x_{2k+1})$ ,  $f_2(x_2, \dots, x_{2k+1})$  - бент функції 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 трьох булевих функцій над  $V_{2k}$  де  $k \geq 1$ , виконують згідно з виразом

$$g(x_1, x_2, \dots, x_{2k}) = x_1(f_1(x_3, \dots, x_{2k}) \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k}), \oplus x_2(f_1(x_3, \dots, x_{2k}), \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k}), \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k})),$$

де  $f_1(x_3, \dots, x_{2k})$ ,  $f_2(x_3, \dots, x_{2k})$  - бент функції 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, має нелінійність  $N_g \geq 2^{2k} - 2^k$  та алгебраїчний степінь кожної координати  $\deg(g) = (\deg(f_1(x)) = \deg(f_2(x))) + 1 = \deg(g, x)$ ,  $i = 1, \dots, 2k + 1$  Функція  $g$  над  $V_{2k}$  є збалансованою функцією, має нелінійність  $N_g > 2^{2k-1} - 2^k$  та алгебраїчний степінь кожної координати  $\deg(g) = (\deg(f_1(x)) = \deg(f_2(x))) + 1 = \deg(g, x)$ ,  $i = 1, \dots, 2k$

Таким чином, виконання процедури конкатенації булевих функцій за допомогою запропонованих виразів дозволяє скоротити час, потрібний для побудови високонелінійних збалансованих булевих функцій над  $V_{2k}$  в 2 рази за рахунок побудови лише двох бент функцій, та підвищити стійкість до атаки криптоаналізу методом диференціалів вищих порядків за рахунок контролю алгебраїчного степеня кожної координати

Спосіб побудови високонелінійних збалансованих булевих функцій над  $V_{2k+1}$  з контролюємим алгебраїчним степенем кожної координати може бути реалізований таким чином Виконується побудова бент функції  $f_1(x_2, \dots, x_{2k+1})$ , над  $V_{2k}$  таким чином, що обирається довільна квадратична бент функція з додаванням нелінійного доданку виду  $x_2 x_4 \dots x_{2k}$  та рахується кількість "0" та "1" в її вихідній послідовності Виконується побудова бент функції  $h(x_2, \dots, x_{2k+1})$  над  $V_{2k}$  таким чином, що обирається довільна квадратична бент функція з додаванням нелінійного доданку виду  $x_3 x_5 \dots x_{2k}$  Далі випадково обирається неконстантна афінна функція  $h(x_2, \dots, x_{2k+1})$ , над  $V_{2k}$  та рахується кількість "0" та "1" в вихідній послідовності конкатенації функцій  $f_2 \oplus h$  Якщо кількість "0" та "1" в вихідній послідовності  $f_1$  дорівнює кількості "0" та "1" в вихідній послідовності  $f_2 \oplus h$ , то функція  $h$  комплементується одиницею  $h = h \oplus 1$ , інакше - не комплементується Після визначення  $f_1$ ,  $f_2$  та  $h$  виконується застосування процедури побудови високонелінійних збалансованих булевих функцій над  $V_{2k+1}$  згідно з виразом

$$g(x_1, x_2, \dots, x_{2k+1}) = x_1(f_1(x_2, \dots, x_{2k+1}) \oplus f_2(x_2, \dots, x_{2k+1}), \oplus h(x_2, \dots, x_{2k+1}), \oplus f_2(x_2, \dots, x_{2k+1}), \oplus h(x_2, \dots, x_{2k+1})),$$

Результатом застосування є функція  $g$  з високими криптографічними показниками стійкості Над  $V_{2k}$  побудова високонелінійних збалансованих булевих функцій з контролюємим алгебраїчним степенем кожної координати може бути реалізована таким чином Виконується побудова бент функції  $f_1(x_3, \dots, x_{2k})$  над  $V_{2k-1}$  таким чином, що обирається довільна квадратична бент функція з додаванням нелінійного доданку виду  $x_3 x_5 \dots x_{2k-1}$  та рахується кількість "0" та "1" в її вихідній послідовності Виконують

нується побудова бент функції  $f_2(x_3, \dots, x_{2k})$  над  $V_{2k-1}$  таким чином, що обирається довільна квадратична бент функція з додаванням нелінійного доданку виду  $x_4 x_6 \dots x_{2k}$ . Далі виконується побудова випадкової неконстантної афінної функції  $h(x_3, \dots, x_{2k})$  над  $V_{2k-1}$  та рахується кількість "0" та "1" в вихідній послідовності конкатенації функцій  $f_2 \oplus h$ . Якщо кількість "0" та "1" в вихідній послідовності  $f_1$  дорівнює кількості "0" та "1" в вихідній послідовності  $f_2 \oplus h$  то функція  $h$  комплементується одиницею  $h = h \oplus 1$ ,

інакше - не комплементується. Після визначення  $f_1$ ,  $f_2$  та  $h$  виконується застосування процедури побудови високонелінійних збалансованих бупевих функцій над  $V_{2k}$  згідно з виразом

$$g(x_1, x_2, \dots, x_{2k}) = x_1(f_1(x_3, \dots, x_{2k}) \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k}), \oplus x_2(f_1(x_3, \dots, x_{2k}), \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k}), \oplus f_2(x_3, \dots, x_{2k}), \oplus h(x_3, \dots, x_{2k})).$$

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