ПРОТИСТОЯННЯ ДИФЕРЕНЦІЙНОМУ І ЛІНІЙНОМУ КРИПТОАНАЛІЗУ ЗБАЛАНСОВАНИМИ НЕЛІНІЙНИМИ БУЛЕВИМИ ФУНКЦІЯМИ

Бевз О.М., Квєтний Р. Н.
Вінницький державний технічний університет,
кафедра автоматики та інформаційно-вимірювальної техніки
E-mail:abevz@aime.vstu.vinnica.ua

Abstract. ***Bevz O. M., Kvetny R. N. Opposition differential and linear cryptanalysis by balanced nonlinear boolean function***. *In this article was offered the boolean functions are appropriated of the properties for the effective opposition of the powerful attack on the contemporary symmetric-key cipher.*

Актуальність. Зростання об`ємів передавання, обробки і зберігання інформації в сучасному інформаційному світі, існування великої кількості користувачів обчислювальних систем і мереж приводять до збільшення кількості спроб несанкціонованого доступу до конфіденційної інформації. Перевірений засіб захисту інформації від несанкціонованого доступу — шифрування інформації по певним алгоритмам з застосуванням ключа, який визначає ступінь секретності. Цим займається криптографія. З іншого боку криптоаналіз намагається розкрити зашифровану інформацію без знання ключа по певним властивостям і закономірностям шифрувальних алгоритмів. Криптографія під впливом криптоаналізу висуває все нові вимоги до математичних перетворень, що застосовуються в шифрувальних алгоритмах. Диференційний[1] і лінійний[2] криптоаналіз — надпотужні засоби для розкриття шифрів, особливо для схем, які базуються на схемі Фейстеля і використовують підстановочно-перестановочні операції, а також для однобічних хеш-функцій. Одним з засобів протистояння диференційному і лінійному криптоаналізу є вимога застосування нелінійних перетворень [3,4] в блоці підстановки (S-боксі). Разом з деякими придатними властивостями до протидії диференційному і лінійному криптоаналізу ці перетворення мають два основних недоліки. Перший — ці перетворення (функції) базуються на обчисленні полінома в кінцевих полях і відповідно мають однакову кількість вхідних і вихідних біт, а широко застосовані блочні шифри

мають кількість вихідних бітів меншу за кількість вхідних, і тому їх застосування не можливе. Відкидання зайвих компонентів функції для відповідності кількості вхідних-вихідних бітів приведе до втрати стійкості шифру. Другий недолік — ці функції не відповідають суворому лавинному критерію (strict avalanche criterion-SAC)[5] і критерію розповсюдження (propagation criterion)[6], що розглядаються як необхідні умови для побудови сучасних шифрів. Таким чином, створення функцій, які одночасно задовольняють критеріям нелінійності, SAC та критерію розповсюдження є актуальною.

Мета досліджень. Мета цієї статті — побудова функцій, що відповідають переліченим вище критеріям. Як відомо з [7,8] цим критеріям відповідають бент-функції, але їх пряме застосування в криптографії неможливе через їхню незбалансованість. Згідно з [9] — збалансованість необхідна умова до функцій, які використовуються для захисту інформації. В статті розроблена збалансована функція, яка має максимально можливу нелінійність і достатньо високу ступінь критерію розповсюдження. Ця функція, представляє собою суму афіної функції $y(x)=x_1$ і будь-якої бент-функції $z(x_2...x_n)$:

$$f(x_1..x_n)=x_1 \oplus z(x_2...x_n)$$

Основні визначення. Функція $f(x)$ — булева, якщо приймає значення 0 чи 1 і її аргументом є послідовність $x=(x_1...x_n)$, де $x_i \in GF(2)$. Вага Хемінга послідовності (вектора) α (0,1) $W(\alpha)$ — це кількість одиниць в векторі α. Функція $y(x_1...x_n)$, де n-кількість вхідних аргументів, має назву афіна, якщо вона задається рівністю $y(x_1...x_n)=a_1x_1 \oplus a_2x_2 \oplus ... \oplus a_nx_n \oplus b$, де a_i, $b \in GF(2)$, $i=1, 2,...,n$. Якщо v– послідовність з довжиною m і u–послідовність з довжиною l, то їх декартовий добутком буде послідовність довжиною ml: $v \otimes u=(v_1u\ v_2u...v_mu)$, де v_i, $i=1..m$, це елемент послідовності v[10]. Скалярним добутком двох векторів $v=(v_1...v_n)$ і $u=(u_1...u_n)$ позначається операція $\langle vu \rangle = v_1u_1 \oplus ... \oplus v_nu_n$, де операції додавання і добутку відбуваються в GF(2).

Бент-функцією $f(x)$ від n аргументів (координат) називається функція, яка задовільняє рівність:

$$2^{\frac{-n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1$$

для будь-якого вектору β, який має довжину n, де вираз $x \in Vn$, означає будь-який вектор $x=(x_1... x_n)$. Бент-функція має наступні властивості [7,8]:

(1) $f(x)\oplus f(x\oplus a)$ — збалансована для будь-якого ненульового вектору $a \in Vn$.

(2) Нелінійність N бент-функції $f(x)$ з n-координатами є максимальною серед функцій, які мають таку ж саму кількість координат і складає $2^{n-1}-2^{(1/2)n-1}$.

(3) Функція $h(x)=f(x)\oplus g(x)$, де $g(x)$ будь-яка афіна функція, також бент-функція.

Булева функція $f(x)$ з n — вхідними бітамі задовольняє SAC по відношенню до ненулевого вектора, якщо при зміні одного вхідного біта ймовірність того, що кожний вихідний біт зміниться, складає ½ для всіх можливих вхідних векторів, а саме функція $f(x)\oplus f(x\oplus a)$ збалансована для будь-якого бітового вектора a з довжиною n, вага Хемінга якого складає 1 [5]. Булева функція задовольняє критерію розповсюдження порядка k, якщо кожний вихідний біт зміниться з ймовірністю ½ , коли k або менше вхідних біт зміниться, а саме функція $f(x)\oplus f(x\oplus a)$ збалансована для будь-якого бітового вектора a з довжиною n, вага Хемінга якого $W(a)$ задовольняє нерівності $1\le W(a)\le k$ [6]. Тобто SAC — це критерій розповсюдження порядка 1.

Збалансованість функції визначається з наступного. Нехай є функція f, аргумент якої є бітова послідовність $V_n=(v_1,...,v_n)$, де кожне v_i приймає значення 0 чи 1, і яка приймає значення 0 чи 1. Тоді (0,1) — послідовність, визначена як $(f(a_0), f(a_1)..., f(a_2n_{-1}))$, має назву таблиця істинності f, де a_i, $0\le i\le 2^n-1$, позначається бітова строка V_n , яка визначає значення числа i в двійковій системі. Послідовність (1,–1), визначена як $((-1)^{f(a0)}, (-1)^{f(a1)},..., (-1)^{f(a2n-1)})$ — має назву послідовність f. Функція f має назву збалансована якщо її послідовність (1,–1) має однакову кількість одиниць і мінус одиниць.

**Розв`язання задачі**. Розв`язання задачі представимо в двох частинах. В першій частині сформулюємо теорему, в якій стверджується що функція $f(x_1..x_n)$ — збалансована, нелінійна і відповідає критерію розповсюдження для всіх вхідних векторів за винятком одного, доведемо її істинність. В другій частині з використанням афіного перетворення вхідних координат перетворимо функцію $f(x_1..x_n)$ в функцію з ступінем критерію розповсюдження n–1, де n — довжина вхідного вектора.

Теорема. Функція $f(x_1..x_n)=x_1\oplus z(x_2...x_n)$, де $z(x_2...x_n)$ — будь-яка бент-функція, задовольняє критерію розповсюдження по відношенню до всіх векто-

рів довжини n за винятком вектору α=(10..0), збалансована, і має нелінійність $N=2^{n-1}-2^{(1/2)n-1}$.

Доведення. Нехай вектор $\alpha=(\alpha_1...\alpha_n)$, $\alpha_1\neq1$, вектор $x=(x_1...\ x_n)$. Тоді $f(x)\oplus f(x\oplus\alpha)=x_1\oplus z(x_2...x_n)\oplus x_1\oplus\alpha_1\oplus z(x_2\oplus\alpha_2...x_n\oplus\alpha_n)=\alpha_1\oplus z(x_2...x_n)\oplus z(x_2\oplus\alpha_2...x_n\oplus\alpha_n)=z(x_2...x_n)\oplus z(x_2\oplus\alpha_2...x_n\oplus\alpha_n)$, згідно властивості (1), ця функція збалансована для будь-якого вектору крім вектора $(\alpha_2...\alpha_n)$=(0..0). Об`єднавши виключення $\alpha_1\neq1$ і $(\alpha_2...\alpha_n)$=(0...0) отримаємо $\alpha\neq$(10...0). Таким чином, $f(x_1...x_n)$ відповідає критерію розповсюдження для будь-якого вектору окрім вектору $\alpha\neq$(10...0).

Очевидно, що послідовність ε будь-якої суми функцій $y(xz)=f_1(x_1...x_n)\oplus f_2(z_1...z_n)$ є послідовність $\varepsilon=\varepsilon_1\otimes\varepsilon_2$, де ε_1 — послідовність $f_1(x_1...x_n)$, ε_2 — послідовність $f_2(z_1...z_n)$; ε — буде мати мати однакову кількість 1 і–1 в випадку, коли або ε_1 — має таку властивість або ε_2, тобто коли або f_1, або f_2 збалансовані. В нашому випадку збалансована функція $f_1(x)=x_1$. Таким чином, $f(x_1..x_n)$ — збалансована.

Згідно властивості (3), функція $f(x_1..x_n)=x_1\oplus z(x_2...x_n)$ — бент функція, так як по умові $z(x_2...x_n)$ — бент функція, а $f_1(x)=x_1$ — афіна функція, тому нелінійність $f(x_1..x_n)$ складає $2^{n-1}-2^{(1/2)n-1}$. *Теорема доведена.*

Так як функція $f(x_1..x_n)$ не відповідає властивості (1) (вона не виконується для всіх векторів, в яких вага Хемінга дорівнює 1), то ступінь її критерію розповсюдження дорівнює нулю і її практичне застосування недоцільно. Ступінь критерію розповсюдження можливо підвищити при застосуванні афіного перетворення координат[11], що виключає виникнення вектору (10..0) для всіх векторів вага Хемінга, яких менше за n (тоді крітерій розповсюдження буде мати ступінь n–1).

Згідно лінійній алгебрі будь-який вектор $x=(x_1...\ x_n)$, може бути перетворений в заданий вектор $y=(y_1...y_n)$ за допомогою одної єдиної невиродженої матриці A з порядком n: $y=x$A. Так перетворення вектору x=$(x_1...\ x_n)$ в такий самий вектор $y=(x_1...\ x_n)$ задається одиничною матрицею A порядку n:

$$\begin{vmatrix} 10.....0_n \\ 01.....0_n \\ ..... \\ 0....1_{n-1}0 \\ 00.....1_n \end{vmatrix} *[x_1...\ x_n]=[x_1...\ x_n]$$

В разі заміни вектора α=(10..0_n), який є винятком в теоремі, на вектор γ=(11..1_n) функція $f(x_1..x_n)$ збереже свої властивості і, таким чином, критерій розповсюдження буде виконуватися для всіх векторів окрім вектору, що знахо-

диться на місці попереднього вектора α - вектору γ=(11..1$_n$). Це означає, що $f(x_1..x_n)$ задовольняє критерію розповсюдження для будь якого вектору з вагою Хемінга n-1 і має ступінь критерію розповсюдження n-1. Згідно цього, координати функції $f(x_1..x_n)$ отримають наступний вигляд:

$$\begin{vmatrix} 11.....1_n \\ 01.....0_n \\ ..... \\ 0....1_{n-1}0 \\ 00.....1_n \end{vmatrix} *[x_1... x_n]=[x_1 (x_1 \oplus x_2)(x_1 \oplus x_3)... (x_1 \oplus x_n)]$$

Отож функція $f(x)=x_1 \oplus z(x_1 \oplus x_2.. x_1 \oplus .x_n)$, де $z(x_1 \oplus x_2.. x_1 \oplus .x_n)$ — бент-функція, задовольняє критерію розповсюдження ступінню n–1.

Приклад застосування. В якості прикладу розглянемо функцію $f(x)=x_1 \oplus z(x)$, де $z(x)$ — бент-функція від 6 змінних $z(x)=x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_2x_4x_6$. Тоді функція $f(x)=x_1 \oplus z(x_1 \oplus x_2.. x_1 \oplus .x_n)$ буде мати вигляд:

$$f(x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7)= x_1 \oplus z(x_1 \oplus x_2\, x_1 \oplus x_3\, x_1 \oplus x_4\, x_1 \oplus x_5\, x_1 \oplus x_6\, x_1 \oplus .x_7)=$$
$$= x_1 \oplus (x_1 \oplus x_2)(x_1 \oplus x_3) \oplus (x_1 \oplus x_4)(x_1 \oplus x_5) \oplus (x_1 \oplus x_6)(x_1 \oplus x_7) \oplus \quad (1)$$
$$\oplus (x_1 \oplus x_3)(x_1 \oplus x_5)(x_1 \oplus x_7)$$

Для для шифрування 1-го біту з застосуванням функції (1) буде необхідно 14 операцій додавання по модулю 2 і 5 операцій множення, що підтвержує невисоку складність її реалізації в програмному і апаратному варіантах. Для порівняння, прийнятий в якості стандарту шифрування, шифр AES[12] в S-боксі для шифрування одного біта застосовує 10 операцій множення, 10 додавання і 2 операції бітового зсуву.

Висновки. Запропонована функція, утворена за допомогою суми афіної функції $y(x)=x_1$ і бент-функції $z(x)=z(x_1 \oplus x_2...x_1 \oplus .x_n)$, яка має ступінь нелінійності $N=2^{n-1}-2^{(1/2)n-1}$. Доведено її збалансованість і відповідність критерію розповсюдження ступіню n–1, де n — кількість аргументів функції. Реалізація функції має невисоку ступінь складності. Застосування функції (1) в S-боксах блочних шифрів підвищить їх стійкість до лінійного і диференційного криптоаналізу. Функція (1) може бути достатньо просто реалізована як в апаратному, так і програмному варіантах. В програмному варіанті доцільно реалізувати функцію (1) в S-боксі, який на вхід отримає один байт відкритого тексту, байт ключа, а на виході одержується зашифрований байт. В такій реалізації функція (1) приймає кожний вхідний біт байту як координату x_1, перетворює її за допомогою 6 бітів ключа, які

є координатами $x_2...x_7$, а інші два біта використовуються для перевірки на парність чи непарність або для іншої службової інформації (це робить можливим застосування такого підходу в телекомунікаційних системах і мережах).

Література

1. M. Matsui. Linear cryptanalysis method for DES cipher. Advances in Cryptology: Proceeding of EUROCRYPT' 93, Springer-Verlag, Berlin, 1993, p.386–397.
2. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1), p.3–72.
3. C. M. Adams and S.E. Tavares. The structured design of cryptographically good S-boxes. Journal of Cryptology, 1990, 193(1), p.27–41.
4. J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. IEE Proceedings, Part E, 1988, 135(6), p.325–335.
5. A. F. Webster and S. E. Tavares. On the design of S-boxes. Advances in Cryptology: Proceedings of CRYPTO `85, Springer-Verlag, Berlin, 1986, p.523–534.
6. B. Preneel, W. Van Leekwijk, Van Linden, R. Goevarts, and J. Vanderwalle. Propogation characteristics of boolean functions. Advances in Cryptology: Proceedings of EUROCRYPT `90, Springer-Verlag, Berlin, 1991, p.161–173.
7. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. Теория кодов, исправляющих ошибки. — Москва: «Связь», 1979. — 744 с.
8. J.F. Dillon. A survey of bent function. The NSA Technical Journal, 1972, p.191–215.
9. S. W. Golomb. Deep space range measurements. Jet Propulsion Laboratory, Pasadena, CA Research Summary, 1960 No. 36-1.
10. В. А. Горбатов. Основы дискретной математики. — Москва: «Высшая школа», 1986. — 311 с.
11. Н. С. Пискунов. Дифференциальное и интегральное исчисление. — Москва: «Наука», 1976. — 575 с.
12. J. Daemen, V.Rijmen, The Block Cipher Rijndael, Springer-Verlag, ISBN 3-540-42580-2.

Здано в редакцію: .03.2003р.

Рекомендовано до друку: д.т.н., проф. Зорі А.А.