УДК 004.056.55(511.88)

ЕФЕКТИВНА МЕТОДИКА ОТРИМАННЯ БУЛЕВИХ ФУНКЦІЙ ДЛЯ КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ

Ю. М. Виноградов[1, a], І. М. Скабенок[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі запропонована проста і ефективна методика автоматизованої генерації булевих функцій, що мають високу нелінійність і відповідають критерії чіткого лавинного ефекту - характеристик, що визначають можливість їх використання в криптографії. Детально описана методика, наведено приклад синтезу булевої функції з її використанням. Запропонована методика оперує з алгебраїчною нормальною формою функції, не накладає обмежень на кількість функцій і потребує незначних обчислювальних ресурсів.

Ключові слова: булеві функції, криптографічні властивості, лавинний ефект, диференційна ентропія

Вступ

Динамічний розвиток та поглиблення інформаційної інтеграції, як одного з найбільш дієвих чинників прогресу суспільства в сучасних умовах, значною мірою залежить від ефективності реалізації функцій захисту інформації та розподілення прав доступу до інформаційних ресурсів.

Домінуючою складовою в арсеналі сучасних засобів захисту інформації є криптографічні перетворення. В теоретичному плані, в основі всіх криптографічних механізмів незворотні математичні перетворення. Одним з найбільш поширеним в сучасній криптографії класом незворотних перетворень є нелінійні булеві перетворення. Вони лежать в основі блокових симетричних алгоритмів шифрування, таких як DES, AES, а також хеш-алгоритмів, таких як SHA, RIPEMD-160 [1]. Ефективність використання булевих функціональних перетворень в криптографії визначається їх диференційними властивостями та нелінійністю.

Тому виникає задача отримання булевих функцій з високими показниками нелінійності та диференційної ентропії.

1. Постановка задачі

Основними специфічними властивостями булевих функцій, що визначають їх ефективність для побудови незворотних перетворень криптографічних алгоритмів є нелінійність та значення диференційної ентропії [1, 2].

Булева функція $f(x_1, ..., x_n)$ задовольняє критерію максимуму диференційної ентропії, або критерію чіткого лавинного ефекту (SAC), якщо зміна значення будь-якої однієї з n змінних призводить до зміни значення функції з вірогідністю 0.5:

$$\forall x_j, j = 1, ..., n : \sum_{x_1,...,x_n \in Z} f(x_1, ..., x_j, ..., x_n) \bigoplus \bigoplus f(x_1, ..., \bar{x_j}, ..., x_n) = 2^{n-1}$$

Нелінійність $N(f)$ булевої функції $f(x_1, x_2, ..., x_n)$ визначається як мінімальна кількість наборів $2n$ можливих значень її змінних в яких вона відрізняється від лінійної функції від n змінних [2].

Найбільш важливими критеріями якості методик одержання балансних булевих SAC-функцій з точки зору їх практичного застосування є:

- витрати обчислювальних ресурсів (машинного часу та пам'яті) на реалізацію процесу синтезу;
- кількість функцій від n змінних, що можуть бути синтезованими;

Вважаючи на важливість проблеми автоматизованого синтезу балансних SAC–функцій для сучасних інформаційних технологій, в останнє десятиліття запропоновано низку підходів до розв'язання цієї проблеми [2, 3].

Виконаний огляд методів синтезу [3, 4], який показав, що опубліковані методи синтезу не в повній мірі відповідають сформульованим вище критеріям і тому актуальним є розробка більш ефективних формальних методів синтезу функцій, що відповідають критерію максимуму повної та диференційної ентропії.

Ціллю дослідження є розробка методики отримання АНФ високо нелінійних SAC-функцій, що має невелику обчислювальну складність, не накладає обмежень на кількість змінних і дозволяє синтезувати велику кількість функцій.

2. Методика побудови АНФ булевої SAC-функції

Сутність запропонованого методу одержання АНФ булевої балансної функції $f(x_1, x_2, ..., x_n)$, що відпо-

[a] vinograd@comsys.kpi.ua

відає критерію чітко лавинного ефекту полягає у виконанні наступної послідовності дій:

1) Множина змінних $\{x_1, ..., x_n\}$ поділяється на чотири підмножини, які не перетинаються $\Lambda \cup \Theta \cup Y \cup \Omega = \{x_1, ..., x_n\}$, $\Lambda = \{x_1, ..., x_{t+1}\}$, $\Theta = \{x_{t+2}, ..., x_{2t+1}\}, Y$ і Ω так, щоб, число змінних, які складають множину $\Lambda - N(\Lambda) = t+1, N(\Omega) = t, \geq 1, N(Y) < N(\Theta)$, а множини Y і Ω можуть бути порожніми.
2) Формується АНФ булевої функції $\varphi(x_1, ..., x_{2t+1})$ у вигляді:

$$\varphi(x_1, x_2, ..., x_{2t+1}) = \bigoplus_{j=1}^{t} x_j \cdot x_{j+t+1} \bigoplus \bigoplus_{k=t+2}^{2t+1} x_{t+1} \cdot x_k$$

3) Формується булева функція $\beta(x_1, ..., x_{t+1})$ у вигляді суми за модулем два непарного числа не константних термів від змінних $x_1, ..., x_{t+1}$ множини Λ.
4) Якщо $Y \neq \emptyset$ і $\Omega \neq \emptyset$, то формується булева функція $\gamma(x_{2t+2}, ..., x_n)$ у вигляді суми за модулем 2 множини Ψ добутків змінних, що належить множині Y на змінні, які належать множині Ω, причому, кожна змінна множин Y та Ω має увійти в якості співмножника хоча б в один з добутків множини Ψ. Якщо $Y \neq \emptyset$, то функція $\gamma(x_{2t+2}, ..., x_n) = 0$.
5) Формується булева функція $\eta(x \in Y, x \in \Omega)$ у вигляді суми за модулем 2 множини Δ добутків змінних множини Λ на змінні множин Ω, причому змінна множини Ω має увійти в парне число добутків множини Δ. Формування функцій $\gamma(x_{2t+2}, ..., x_n)$ і $\eta(x \in Y, x \in \Omega)$ має бути здійснене таким чином, що у добутки, які складають множини Ψ і Δ увійшла б кожна змінна множини Ω. Якщо $\Omega \neq \emptyset$, то $\gamma(x_{2t+2}, ..., x_n) = 0$ і $\eta(x \in Y, x \in \Omega) = 0$.
6) АНФ балансної SAC-функції $f(x_1, ..., x_n)$ формується у вигляді:

$$f(x_1, ..., x_n) = \varphi(x_1, ..., x_{2t+1}) \bigoplus \bigoplus \beta(x_1, ..., x_{t+1}) \bigoplus \gamma(x_{2t+2}, ..., x_n) \bigoplus \bigoplus \eta(x \in Y, x \in \Omega)$$

Властивості балансності і SAC сформованої у відповідності з викладеним методом не зміняться, якщо до неї додати за модулем 2 наступні функції:

- довільну функцію $\delta(x \in Y)$, визначену на змінних множини Y;
- довільну функцію $\rho(x \in \Omega)$, визначену на змінних множини Ω;

Доведено, що нелінійність $N(f)$ сформованої за запропонованим методом булевих функцій $f(x_1, ..., x_n)$ визначається формулою:

$$N(f) \geq 2^{n-1} - 2^{n/2}, \texttt{для парних n}$$
$$N(f) \geq 2^{n-1} - 2n - (n-1)/2 - 1 =$$
$$= 2^{n-1} - 2^{n+1/2-1}, \texttt{для непарних n}$$

Запропонований метод може бути ілюстровано наступним прикладом синтезу булевої SAC-функції від 6-ти змінних. Відповідно $n = 6$. Вибирається значення $t = 2$, відповідно $\lambda = \{x_1, x_2, x_3\}$ і $\omega = \{x_4, x_5\}$. Довільно вибираються множини $Y \neq \emptyset$ та $\Omega = x_6$. Відповідно до п.2 формується функція $\varphi(x_1, x_2, x_3) = x_1 \cdot x_4 \bigoplus x_2 \cdot x_5 \bigoplus x_3 \cdot x_4 \bigoplus x_3 \cdot x_5$. Відповідно до п.3 функція β формується у вигляді $\beta = x_1 \cdot x_2 \cdot x_3$. У відповідності з п.4 і п.5 $\gamma = 0$ та $\eta = x_2 \cdot x_6 \bigoplus x_3 \cdot x_6$. Згідно з п.6 функція $f(x_1, ..., x_6) = x_1 \cdot x_4 \bigoplus x_2 \cdot x_5 \bigoplus x_3 \cdot x_4 \bigoplus x_3 \cdot x_5 \bigoplus x_2 \cdot x_6 \bigoplus x_3 \cdot x_6 \bigoplus x_1 \cdot x_2 \cdot x_3$. Неважко переконатися, що синтезована функція відповідає SAC-критерію і її нелінійність дорівнює 26.

Головні переваги запропонованої методики у порівнянні з відомими полягають у її простоті, можливості синтезу SAC-функцій від великої кількості змінних, а також у більшій кількості функцій, що можуть бути утворені.

Висновки

В результаті проведених досліджень запропоновано просту методику побудови булевих функцій, що мають важливі для криптографічних застосувань властивості: відповідність критерію лавинного ефекту та високу нелінійність, близьку до теоретичного максимуму для балансних функцій. Вказані властивості функцій забезпечують високий рівень здатності алгоритмів, побудовані на них протистояти лінійному та диференційному аналізу.

Перелік використаних джерел

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М. :,Триумф, 2002. — 816 с.
2. Forre R. The strict avalanche criterion: spectral properties of Boolean functions and extend definition // Advanced in Cryptology – Crypto'88 Proceeding, Lecture Notes in Computer Sciences, 403 — 1990 — p. 450-468
3. Kurosawa K., Satoh T. Design of SAC/PC(l) of Order k Boolean Functions and Three Other Cryptographic Criteria. //Proc. International Conf. Advanced in Cryptology – Eurocrypto'97, LNCS 1233 — 1997 — p. 433-449
4. Maintra S., Pasalic E. Further construction of resilient Boolean functions with very high nonlinearity // IEEE Trans. on Information Theory. — 2002. — Vol. 48, No. 7, 1825-1834 p.