УДК 681.3.06

В.І. Долгов, О.І. Олешко
Харківський національний університет радіоелектроніки,
кафедра БІТ

ОЦІНКА ПОКАЗНИКІВ СТІЙКОСТІ БСШ НА ОСНОВІ АНАЛІЗУ ЗМЕНШЕНИХ МОДЕЛЕЙ ПРОТОТИПІВ

© Долгов В.І., Олешко О.І., 2012

Вдосконалено методи оцінки стійкості блокових симетричних шифрів щодо атак диференційного і лінійного криптоаналізу. Оцінку стійкості виконано на основі вивчення показників і властивостей зменшених моделей прототипів, що дає змогу перевірити відповідність між показниками стійкості шифрів, отриманих доказовим та розрахунковим способами.

Ключові слова: блоковий симетричний шифр, диференційний криптоаналіз, лінійний криптоаналіз, оцінка стійкості.

This work is devoted to improvement of estimation methods of symmetric block ciphers security to the attacks of differential and linear cryptanalysis. Here we develop the method of analysis based estimation of small prototypes model properties. We estimate block ciphers security by investigating characteristics and properties of small model prototypes, thus we check up accordance between theoretical and empirical values of block ciphers security.

Key words: symmetric block cipher, differential cryptanalysis, linear cryptanalysis, block ciphers security estimation.

Вступ

Симетричні шифри сьогодні виступають як один із основних інструментів, що забезпечує криптографічний захист інформації як приватного, так і державного сектору економіки, насамперед в таких критично важливих сферах, як транспорт, фінанси, армія тощо. Блокові симетричні шифри (БСШ) є невід'ємним компонентом сучасних систем криптографічного захисту інформації. Основну область їх використання становлять застосування, що обробляють великі обсяги конфіденційної інформації і висувають серйозні вимоги до продуктивності систем захисту.

Однією з основних вимог, які висуваються до сучасних і перспективних БСШ, є висока стійкість до відомих методів криптоаналізу, насамперед диференційного і лінійного. Конкурси з відбору перспективних блокових шифрів, що відбулися упродовж останнього десятиліття в Україні і в світі, наочно продемонстрували високу складність виконання такої експертизи і необхідність використання значних часових та інтелектуальних ресурсів. Адже за доволі недовгий час необхідно не тільки знайти теоретичні обґрунтування рішенням, які приймаються, але й отримати реальні практичні результати для накопичення фактичних даних і виконання аналізу стійкості.

Під час проведення конкурсу AES використовувалося поняття мінімальних вимог до БСШ, основними з яких є [1]:

1. Криптоалгоритм повинен будуватися з використанням БСШ з довжиною блока $l_б = 128$ біт.

2. Довжина початкових ключів повинна бути lк = 128, 192 і 256 біт.

З усього вищесказаного випливає, що оцінка стійкості БСШ являє собою складну багатокритеріальну задачу. Безумовно, основним критерієм є реальна захищеність від криптоаналітичних атак (криптоалгоритм повинен забезпечувати обчислювальну стійкість за заданої вартості криптоаналізу і вказаних імовірнісно-часових характеристик криптостійкості).

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Використання зменшених моделей БСШ

Як відомо, диференційний і лінійний криптоаналіз належать до найпотужніших атак, тому перевірка захищеності від них є обов'язковою, можна сказати, основною під час оцінцінювання стійкості БСШ. Відомо також, що пряма перевірка захищеності від цих атак не може бути реалізована на практиці, адже повний аналіз сучасного шифру на реальних довжинах вхідного тексту і ключів вимагає використання таких ресурсів пам'яті та обчислень, які нинішня комп'ютерна техніка забезпечити не може.

Для здолання труднощів аналізу повномасштабних алгоритмів шифрування ми пішли шляхом розробки і дослідження зменшених моделей прототипів, для яких буде достатньо обчислювальних ресурсів, що є у нашому розпорядженні. Отримані результати змушують підійти до формування оцінок стійкості до атак диференційного і лінійного криптоаналізу з цілком нових позицій.

Наші дослідження показують, що велика кількість добре відомих алгоритмів шифрування допускає масштабування. Вдається побудувати зменшені моделі, які зберігають усі властивості своїх прототипів і дають змогу виконувати багато завдань щодо аналізу і порівняння за показниками стійкості відповідних повномасштабних версій. Усе вищесказане підтверджує актуальність подальших досліджень у цьому напрямку і висуває його в число перспективних напрямків розвитку і вдосконалення технологій блочного симетричного шифрування.

Шифруючі перетворення як випадкові підстановки

Для блокового шифру простір M відкритих текстів збігається з простором P зашифрованих текстів, тому перетворення шифрування на випадково обраному ключі часто моделюють за допомогою випадкової перестановки (у багатьох джерелах поняття "підстановка" і "перестановка" використовуються як синоніми). Так, наприклад, у [4] є твердження, що блоковий шифр для кожного ключа не повинен відрізнятися від випадкової перестановки.

Багато авторів вивчали випадкові підстановки, і для аналізу якості перетворень типу підстановка в БСШ використовується оцінка кількості інверсій, циклів та зростань порівняно з теоретично розрахованими асимптотичними значеннями. Одними із основних показників стійкості симетричних шифрів до атак диференційного і лінійного криптоаналізу у багатьох роботах розглядаються максимальні значення вірогідностей таблиць XOR різниць і таблиць лінійних апроксимацій шифрів, що розглядаються як випадкові підстановки.

Диференційні властивості випадкових підстановок

Під час розгляду диференційних властивостей випадкових підстановок вважається [2], що $p : Z_2^m \to Z_2^m$ є бієктивним m-бітним відображенням і S_2^m позначає безліч усіх таких відображень, відомих у математичній літературі як симетрична група. Через $\Lambda_p(\Delta X, \Delta Y)$ позначено значення XOR таблиці (її комірки) для пари значень різниць входів і виходів $\Delta X, \Delta Y \in Z_2^m$, $\Delta X = X \oplus X'$, $\Delta Y = p(X) \oplus p(X')$ підстановки $p \in S_2^m$.

Нагадаємо, що таблиця XOR є $2^m \times 2^m$ матрицею, у якої $XOR_p(i, j) = \Lambda_p(i, j)$, $0 \le i, j \le 2^{m-1}$. Для m-бітної підстановки π XOR таблиця має таку загальну форму:

$$XOR_p = \begin{vmatrix} 2^m & 0 & 0 & \mathbf{L} & 0 \\ 0 & a_{1,1} & a_{1,2} & \mathbf{L} & a_{1,2^{m-1}} \\ 0 & a_{2,1} & a_{2,2} & \mathbf{L} & a_{2,2^{m-1}} \\ \mathbb{M} & \mathbb{M} & \mathbb{M} & \mathbf{L} & \mathbb{M} \\ 0 & a_{2^{m-1},1} & a_{2^{m-1},2} & \mathbf{L} & a_{2^{m-1},2^{m-1}} \end{vmatrix} \quad \begin{matrix} def \\ = \end{matrix} \quad \begin{vmatrix} 2^m & 0 \\ 0 & A_p \end{vmatrix}.$$

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Нас цікавитимуть властивості $2^{m-1} \times 2^{m-1}$ підматриці $A_p = \left| a_{i,j} \right|$, $1 \le i, j \le 2^{m-1}$, яка відповідає частині XOR таблиці із входами (комірками), що мають ненульові значення.

Як встановлено, закон розподілу переходів у XOR-таблицях випадкових підстановок розраховується за допомогою виразу

$$\Lambda_{m,2k} = \frac{(2^m - 1)^2}{2^m!} \cdot \left(\begin{matrix} 2^{m-1} \\ k \end{matrix} \right)^2 \cdot k! \cdot 2^k \cdot \Phi(2^{m-1} - k), \quad (1)$$

де підстановка π вибрана рівноімовірно з множини S_2^m і $0 \le k \le 2^{m-1}$, а $\Phi(d)$ обчислюється, як

$$\Phi(d) = (2d)! - \sum_{i=1}^{d} i! \cdot 2^i \left(\begin{matrix} d \\ i \end{matrix} \right)^2 \cdot \Phi(d - i). \quad (2)$$

Формулу (1) можна отримати, враховуючи [2]. Для порівняння теоретичних і експериментальних результатів нас цікавитиме середнє значення максимуму XOR-таблиці, яке ми отримаємо із співвідношення (1) як максимальне значення k, за якого результат розрахунків дає найменше ціле значення – одиницю. У табл. 1 наведені результати порівняння експериментів з випадковими підстановками, і даних, отриманих за формулою (1). Одночасно у табл. 1 наведені результати апроксимації формули (1), для якої запропонована проста оцінка $\Lambda_{m,2k} = m + 4$.

Таблиця 1

Порівняння розрахункових та експериментальних результатів для диференційного криптоаналізу

m	$\Lambda_p(\Delta X, \Delta Y) = 2k$	2k	Експеримент
4	3,379 0,459	6 8	6,7 ≤ (m + 3)
5	3,08 1,708	6 8	7,94 ≤ (m + 3)
6	6,6 0,675	8 10	9,1 ≤ (m + 4)
7	2,641 0,221	10 12	10,3 ≤ (m + 4)
8	0,8748	12	11,4
9	3,474 0,248	12 14	12,5 ≤ (m + 4)
10	13,8495 0,99	12 14	13,4 ≤ (m + 4)
11	3,952 0,247	14 16	14,5 ≤ (m + 4)
12	15,787 0,987	14 16	15,3 ≤ (m + 4)

Властивості таблиць лінійних апроксимацій випадкових підстановок

Для оцінки стійкості шифру до атак лінійного криптоаналізу розв'язується задача визначення явного вигляду закону розподілу зміщень комірок таблиць лінійних апроксимацій випадкових підстановок.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Відзначимо, що близьку за постановкою задачу нам вдалося знайти у роботах Luka O'Connora 1995-го року, в яких наводяться розрахункові співвідношення, які нас цікавлять, але без доведення [3].

Нехай $p: Z_2^n \to Z_2^n$ – бієктивне n-бітне відображення і S_2^n буде множиною усіх таких відображень. Для n-бітного вектора $X \in Z_2^n$ нехай X_i позначає i-й біт вектора X. Лінійна апроксимаційна таблиця для підстановки π позначається LAT_p і є таблицею розміру $2^n \times 2^n$ з елементами $LAT_p(a, b)$, що визначаються співвідношенням:

$$LAT_\pi(\alpha,\beta) \overset{def}{=} \#\left\{ X / X \in Z_2^n, \quad \bigoplus_{i=1}^{n} X[i] \cdot \alpha[i] = \bigoplus_{i=1}^{n} \pi(X[i]) \cdot \beta[i] \right\},$$

де $a, b \in Z_2^n$, а $'\cdot'$ означає операцію побітового І.

Відповідно до наведеного визначення, $LAT_p(a, b)$ являє собою число рівностей парності між лінійною комбінацією вхідних бітів (що визначаються маскою α по входу в LAT_p підстановки за рядками) і лінійною комбінацією вихідних бітів (що визначаються маскою β по входу у таблицю LAT_p підстановки за стовпцями).

Нас цікавитиме теорема, наведена у [3]. Нагадаємо її тут і скористаємося нею для отримання необхідних оцінок.

Теорема 1: Нехай $l(a, b)$ – випадкове число, що відповідає значеню лінійною апроксимаційної таблиці підстановки $LAT_p(a, b)$, коли підстановка π обрана рівноймовірно з множини S_2^n і маски a, b – ненульові. Тоді $l(a, b)$ для цілих значень k, $0 \le k \le 2^{n-1}$ приймає тільки парні значення і ймовірність того, що $l(a, b) = 2k$, визначається так:

$$\Pr\left(l(a, b) = 2k\right) = \frac{\left(2^{n-1}!\right)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ k \end{pmatrix}^2.$$

Очікуване число елементів таблиці лінійних апроксимацій, що мають значення $2k$, обчислюється за формулою

$$E\left[l(p, 2k)\right] = \frac{(2^n - 1)^2 \cdot (2^{n-1}!)^2}{2^n!} \cdot \begin{pmatrix} 2^{n-1} \\ 2^{n-2} + |k| \end{pmatrix}^2, \qquad (3)$$

де підстановка π вибрана рівноімовірно і $|k| \le 2^{n-2}$.

У цьому випадку, як і для формули (1), розраховувалося середнє значення максимуму таблиці лінійних апроксимацій, прирівнюючи (3) до одиниці і шукаючи відповідне максимальне значення k. Результати таких розрахунків разом з експериментальними даними наведені у табл. 2 разом із запропонованою оцінкою $E\left[l(p, 2k)\right] = (3/2)^n$.

В останні роки вчені кафедри БІТ ХНУРЕ розвивають підхід до оцінки стійкості БСШ [5], який полягає у тому, що асимптотичні показники стійкості (максимуми повного диференціала таблиць XOR і максимуми лінійних таблиць) сучасних БСШ, не залежать ні від блоків підстановок, ні від числа циклів шифруючого перетворення, а лише від розміру бітового входу шифру. У процесі досліджень ми підтвердили той факт, що, шифруючи перетворення, фактично повторюють з високою точністю випадкові підстановки.

Отже, основним результатом цієї роботи необхідно вважати отримання аналітичних співвідношень для розрахунку максимальних значень XOR-таблиць і зміщень таблиць лінійних апроксимацій випадкових підстановок, що є справедливими, як показує аналіз, і для зменшених моделей шифрів і для їх прототипів.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Таблиця 2

Порівняння розрахункових та експериментальних результатів для лінійного криптоаналізу

n	2k	$E[l(p,2k)]$	Експеримент
4	4 6 8	3,89 1,118 0,017	5,498 $(3/2)^4 = 5{,}06$
6	12 14 16	9,013 1,7 0,239	14,48 $(3/2)^6 = 11{,}39$
8	32 34	2,12 0,7457	34,68 $(3/2)^8 = 25{,}62$
10	74 76	1,16 0,64	78,8 $(3/2)^{10} = 57{,}66$
12	162 164	1,129 0,82	116,24 $(3/2)^{12} = 130$
14	350 352	1,069 0,900	314 $(3/2)^{14} = 292$
16	748 750	1,027 0,93	720 $(3/2)^{16} = 657$

Висновок

Відтепер ми маємо реальну можливість виконувати оцінку показників безпеки шифрів щодо атак диференційного і лінійного криптоаналізу розрахунковим шляхом, що дуже важливо для своєчасного і якісного проведення експертизи щодо стійкості сучасних БСШ.

1. AES. The Advanced Encryption Standard Development Process [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/encryption/aes/, 1997. 2. O'Connor L. J. On the Distribution of Characteristics in Bijective Mappings / O'Connor L. J. // Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, 1994. - Vol. 795. - T: Hellesethed., Springer-Verlag. - P. 360–370. 3. Luke O'Connor. On Linear Approximation Tables and Ciphers secure against Linear Cryptanalysis. – [Electronic resources] / Luke O'Connor. - 1995. - Режим доступу: http://www.zurich.ibm.com/~oco/pub/LAT_lueven.ps.Z. 4. Borst J. Block Ciphers: Design, Analysis and Side-Channel Analysis / Borst J. // PhD thesis, Dept. Elektrotechniek, Katholieke Universiteit Leuven. – Belgium. – Sep. 2001. 5. Roman Oleinikov, Oleg Oleshko, Konstantin Lisickay Differential properties of random permutations. Proceedings International Conference TCSET'2010, Lviv-Slavske, Ukraine February 23–27. – 2010, p.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua