УДК 621.396

О.О. КУЗНЕЦОВ

Харківський університет Повітряних Сил ім. І. Кожедуба, Україна

ДОСЛІДЖЕННЯ ДИФЕРЕНЦІЙНИХ ВЛАСТИВОСТЕЙ МІНІВЕРСІЙ БЛОЧНО-СИМЕТРИЧНИХ ШИФРІВ AES І ADE

Розглянуто мініверсії блочно-симетричних шифрів: національного стандарту шифрування США AES (Advanced Encryption Standard) (FIPS - 197) та блочно-симетричного шифру ADE (Algorithm of Dynamic Encryption) – кандидата на національний стандарт шифрування України. Досліджуються особливості перевірки стійкості блочно-симетричних шифрів до атак диференційного криптоаналізу для зменшених моделей. Викладається методика статистичних досліджень диференційних властивостей блочно-симетричних шифрів та наводяться результати порівняльних досліджень мініверсій шифрів AES і ADE.

алгоритм блочного симетричного шифрування, диференційний криптографічний аналіз, розподіл різниць, мініверсії шифрів, статистичні дослідження диференційних властивостей

Вступ

Відповідно до рішення Державної служби спеціального зв'язку та захисту інформації в Україні проводиться відкритий конкурс блочних симетричних криптоалгоритмів [1]. Однією з пропозицій є алгоритм шифрування із динамічно керованими криптопримітивами ADE (Algorithm of Dynamic Encryption) [2]. В даній роботі розглядаються криптографічні властивості шифру ADE, оцінюється стійкість до диференційного криптоаналізу у порівнянні із аналогічними характеристиками національного стандарту шифрування США AES.

Диференційні властивості мініверсій шифрів AES і ADE

Сутність диференційного криптоаналізу полягає у використанні специфічних входів в так звані таблиці розподілу різниць S-блоків, що використовуються блочним шифром [3, 4]. Таблиця розподілу різниць S-блоку $n \times s$ – це матриця розміру $2^n \times 2^s$, рядки матриці індексовані векторами, що представляють вхідні різниці, колонки індексовані векторами, що є вихідними різницями. Комірка в таблиці індексована парою входів (α, β) і вказує число пар вхідних векторів що мають вхідну різницю α які переходять у вихідну різницю β. Таблиця дозволяє знайти найбільш вірогідні значення переходів вхідної різниці у вихідну, які використовуються для побудови відповідних одноциклових диференційних характеристик.

Атака диференційного криптоаналізу здійснюється шляхом пошуку диференційних характеристик, які дозволяють фіксовану вхідну різницю довести з ймовірністю, більшою, ніж дає атака прямого перебору ключів, до фіксованої різниці на вході передостаннього циклу. Якщо таку характеристику вдається знайти, то на основі вивчення статистики проходження пар відібраних відкритих текстів через останній цикл шифрування будується процедура визначення ключових біт шифру.

Оскільки диференційний криптоаналіз відновлює біти ключа на останньому циклі, то для успішної атаки на шифр необхідний багатоцикловий диференціал (диференційна характеристика), який покриває майже всі цикли шифру і має вірогідність, яка значно перевищує значення 2^{-n} (тут n – розмір ключа в бітах). Відповідно, за критерій захищеності r-циклового шифру від атак диференційного криптоаналізу вважається виконання нерівності $P^{(r-1-q)} \le 2^{1-n}$, де $q = 1$ або $q = 2$ визначається

можливістю реалізації NR-атаки з різною кількістю циклів (атаки з $N = q$ підібраними завершальними циклами). Значення $P^{(r-l-q)}$ характеризує складність виконання найбільш ресурсоємного етапу диференційного криптоаналізу – підбору правильної пари відкритих текстів. Правильна пара дозволяє припустити значення бітів підключа останнього циклу.

При визначенні стійкості S-блоків до атак диференційного криптоаналізу використовується поняття диференційної δ - рівномірності [3, 4].

Нехай F буде $n \times s$ S-блоком, де $n \geq s$. δ – найбільше значення в диференційній таблиці:

$$\delta = \max_{\alpha \in V_n, \alpha \neq 0} \max_{\beta \in V_s} \left| \{x \left| F(x) \oplus F(x \oplus \alpha) = \beta \} \right| \right|.$$

Тоді S-блок F є диференційно δ -рівномірний. Очевидно, що диференційна рівномірність S-блока міститься в межах $2^{n-s} \leq \delta \leq 2^n$. S-блок вважається за хороший по цьому показнику, якщо значення δ достатньо мале.

По аналогії з цим визначенням розглянемо умовну Δ_k - рівномірність всього набору шифруючих перетворень.

Для блокового симетричного шифру $n = \{K, M, C, T\}$, де K, M і C – кінцеві множини, що позначають ключовий простір, простір повідомлень і простір шифртекстів, а $T : K \times M \to C$ – шифруюче перетворення таке, що для $x \in M$ маємо. Значення

$$\Delta_k = \max_{\alpha \in V_n, \alpha \neq 0} \max_{\beta \in V_s} \left| \{x \left| T_k(x) \oplus T_k(x \oplus \alpha) = \beta \} \right| \right|$$

є умовною Δ_k – рівномірністю шифру.

Отже, сутність виконання атаки диференційного криптоаналізу для зменшених моделей шифрів зводиться до визначення максимального значення кількості переходів фіксованої різності на вході шифру в фіксовану різність на виході шифру.

У проведених дослідженнях в якості S-блока розглядався цілком весь набір шифруючих перетворень для одного ключа, так що загальне число різних підстановок дорівнює потужності ключового простору K, і для зменшених версій шифрів таблиця диференціалів має розмір $2^{16} \times 2^{16}$ (у мініверсіях використовуються 16-бітові блоки даних [5]), тобто можливо 2^{16} варіантів вхідних і стільки ж вихідних різниць.

При проведенні статистичного експерименту побудовано 1000 варіантів таблиць, кожна для випадково вибраного значення 16-бітового ключа шифрування. Визначалися наступні показники:

– середнє по множині з 1000 випадково вибраних ключів шифрування (по множині таблиць) значення Δ^r - рівномірності r-циклового шифру

$$\Delta^r = \frac{1}{1000} \sum_{i=1}^{1000} \Delta_{k_i}^r , \qquad (1)$$

де $\Delta_{k_i}^r$ – значення показника рівномірності (максимальне значення заповнення кожної з таблиць) для r-циклового шифру з ключем шифрування k_i, $r = 2, 4, 6, 8$;

– $\Delta_{k_i}^r$ – рівномірність *r*-циклового шифру при порядковому розгляді таблиць розподілу диференціалів (виконувалося усереднювання значень максимального числа переходів фіксованої вхідної різниці (XOR) відкритих текстів у вихідну різницю відповідних шифртекстів для рядків таблиць диференціалів);

– середньоквадратичне відхилення умовної Δ_k^r - рівномірності для вибірки з 1000 ключів;

– абсолютні значення умовної Δ_k^r - рівномірності *r*-циклового шифру по вибірці з 1000 ключів зашифрування;

– математичне очікування мінімальних значень максимумів числа переходів *r*-циклового шифру.

Оскільки в експерименті брало участь тільки 1000 реалізацій ключів зашифрування, то використовувався метод довірчих інтервалів, що є методом математичної статистики, спеціально призначеним для побудови множини наближених значень невідомих параметрів імовірнісних розподілів.

Таблиця 1

Δ^r - рівномірність r –циклового шифру.

Шифр	Кількість раундів						
	2	3	4	5	6	7	8
babyADE	3254±59	301,3±7,3	20,064±0,348	19,170±0,124	19,120±0,092	19,166±0,093	19,106±0,091
miniAES	4955±24	640,6±4,6	43,066±0,999	20,538±0,202	19,082±0,093	19,122±0,092	19,122±0,096

Таблиця 2

Δ^r - рівномірність r –циклового шифру при порядковому розгляді таблиць розподілу диференціалів.

Шифр	Кількість раундів						
	2	3	4	5	6	7	8
babyADE	61,2±0,5	13,475±0,047	11,3559±0,0006	11,3459±0,0004	11,3456±0,0004	11,3458±0,0004	11,3458±0,0004
miniAES	77,3±0,2	16,103±0,01	11,4065±0,0012	11,3488±0,0004	11,3456±0,0004	11,3458±0,0004	11,3456±0,0004

Таблиця 3

Середньоквадратичне відхилення умовної Δ_k^r - рівномірності для вибірки з 1000 ключів.

Шифр	Кількість раундів						
	2	3	4	5	6	7	8
babyADE	154,9	11,815	1,213	1,209	1,208	1,208	1,208
miniAES	182,2	20,609	1,355	1,211	1,208	1,208	1,208

Таблиця 4

Абсолютні значення умовної Δ_k^r - рівномірності r –циклового шифру по виборці з 1000 ключів шифрування.

Шифр	Кількість раундів						
	2	3	4	5	6	7	8
babyADE	5632	1088	72	40	24	22	26
miniAES	5632	768	108	36	24	24	28

Таблиця 5

Математичне очікування мінімальних значень максимального числа переходів r –циклового шифру.

Шифр	Кількість раундів						
	2	3	4	5	6	7	8
babyADE	16,5±0,2	10,00±0,005	8,93±0,08	8,89±0,08	8,85±0,08	8,91±0,08	8,90±0,08
miniAES	18,6±0,4	10,00	9,01±0,08	8,85±0,08	8,93±0,08	8,92±0,08	8,86±0,08

Нехай $X_1, X_2, \ldots, X_n$, $n \geq 2$ – незалежні випадкові величини, що підкоряються одному і тому ж нормальному закону з невідомими параметрами $EX_i = \theta_1$ і $DX_i = \theta_2$, причому потрібно побудувати інтервальну оцінку $u(\theta) = \theta_1$. Нехай

$$\bar{X} = \frac{1}{n} \cdot \sum_{i=1}^{n} X_i, \quad s^2 = \frac{1}{n-1} \cdot \sum_{i=1}^{n} (X - \bar{X})^2.$$

Випадкова величина $T = \sqrt{n}(\bar{X} - \theta)/s$ підкоряється розподілу Ст‘юдента з $n-1$ ступенями свободи, яке не залежить від невідомих параметрів θ_1 і θ_2 ($\theta_1 < \infty, \theta_2 > 0$), і при будь-якому позитивному t вірогідність події

$$\left\{ \bar{X} - \frac{t \cdot s}{\sqrt{n}} < \theta_1 < \bar{X} + \frac{t \cdot s}{\sqrt{n}} \right\}$$

залежить лише від t. Якщо вказаний інтервал прийняти за інтервальну оцінку для θ_1, то йому відповідатиме довірча ймовірність

$$P_c(\theta_1, \theta_2) = P\{|T| < t\} = 1 - \alpha,$$

що не залежить від параметрів $\theta = \{\theta_1, \theta_2\}$.

В результаті, задаючись довірчою вірогідністю $P_c(\theta_1, \theta_2) = 0,99$, тобто $\alpha = 0,01$, на підставі таблиці розподілу Ст‘юдента для заданих значень α і n = 1000 отримуємо t = 2, 576, і, отже

$$\frac{t \cdot s}{\sqrt{n}} = \frac{2,576 \cdot s}{\sqrt{1000}} = 0,081 \cdot s.$$

Результати статистичних досліджень диференційних властивостей міні-шифрів BABY-ADE і mini-AES приведені в таблицях 1 – 5.

Характеристики, представлені в них, були отримані при обробці 1000 реалізацій таблиць диференціалів. Довірчий інтервал був заданий рівнем значущості $\alpha = 0,01$, що відповідає довірчій вірогідності $P = (1 - \alpha) \cdot 100\% = 99\%$.

Висновки

Представлені результати свідчать, що диференційні властивості шифру BABY-ADE не гірші за диференційні властивості шифру mini-AES. Якщо бути точнішим, то можна відзначити, що введені в шифр BABY-ADE механізми динамічного (ключового) управління привели до невеликого покращання його диференційних властивостей. Представляється, що ці висновки можна перенести і на повні версії шифрів.

В цілому, по представлених результатах можна зробити висновок, що для шифрів AES і ADE складність атаки диференційного криптоаналізу (якби можна було реалізувати атаку на повні диференціали) декілька менше складності атаки повного перебору ключів (для малих версій шифру, судячи за даними таблиці 4, не більше ніж в декілька десятків разів). Якщо це співвідношення зберігається і для великих шифрів, то шифри AES і ADE дійсно є стійкими до атак диференційного криптоаналізу.

Литература

1. Сайт Державної Служби Спеціального зв’язку та захисту України [Електронний ресурс]. – Режим доступу: http://dstszi.gov.ua.

2. Кузнецов А.А., Сергиенко Р.В., Наумко А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) // Прикладная радиоэлектроника. – 2007. – Т. 6. № 2. – С. 241-249.

3. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems // The Weizmann Institute of Science, Israel – July 19, 1990 [Електронний ресурс]. – Режим доступу: http://citeseer.ist.psu.edu

4. K.Nyberg, L. Rnudsen, "Provable Security Against Differential Cryptanalysis" // Proc. of Crypto ′92. – Springer-Verlag, 1998. – P. 566-574.

5. Кузнецов А.А., Онищенко В.В., Сергиенко Р.В. Исследование дифференциальных характеристик шифра BABYADE // Проблеми інформатики і моделювання. – Х.: НТУ „ХПІ”. – 2007. – С. 12.

Надійшла до редакції 30.05.2008

Рецензент: д-р фіз.-мат. наук, проф. В.В. Погосов, Запорізький національний технічний університет, Запоріжжя.