УДК 621.391:519.2

С.М. КОНЮШОК, канд. техн. наук

ДОСЛІДЖЕННЯ k-ВИМІРНОСТІ БУЛЕВОЇ ФУНКЦІЇ ШИФРУ LILI-128

Вступ

Атаки на основі відібраних векторів ініціалізації відносять до найбільш потужних атак на синхронні потокові шифри (СПШ). Зокрема, кубічна атака [1], статистична атака FKM [2], а також їх різноманітні модифікації та вдосконалення [3 – 8]. До будь-якого криптографічного алгоритму, який можливо описати за допомогою булевої функції $F:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to\{0,1\}$ (один з аргументів якої є секретним, а другий – загальнодоступним параметром), застосовуються подібні атаки. Для СПШ, в якості F (наприклад, функція ключа $k\in\{0,1\}^{l_0}$ та вектора ініціалізації $c\in\{0,1\}^{l_1}$) можливо обрати знак вихідної послідовності генератора гами шифру в певному такті. Слід зауважити, що функція F вважається доступною зловмиснику в вигляді оракула ("чорної скрині"), зокрема, може бути невідомим алгоритм, який реалізує цю функцію.

На етапі попередніх обчислень зловмисник може подавати на вхід оракула будь-які пари векторів $(x,y)\in\{0,1\}^{l_0}\times\{0,1\}^{l_1}$, обчислюючи значення $F(x,y)$, щоб зібрати потрібну інформацію про властивості функції F. Потім зловмисник отримує доступ до оракулу $F_k(c)=F(k,c)$, $c\in\{0,1\}^{l_1}$, де значення ключа $k\in\{0,1\}^{l_0}$ невідоме. Зловмисник може обирати будь-які вектори $c\in\{0,1\}^{l_1}$ та обчислювати значення $F_k(c)$ при фіксованому ключі k, спрямовуючи зусилля на відновлення цього ключа (або отримати про нього деяку інформацію). Іншою можливою стратегією зловмисника є побудова розрізняючої атаки, спрямованої на те, щоб статистично відрізнити (за прийнятний час з достатньо високою надійністю) відображення F_k від випадкового рівноімовірного відображення $\Phi:\{0,1\}^{l_1}\to\{0,1\}$ [3, 4].

Атака FKM [2] базується на основі статистичного наближення функції F булевою функцією g, що залежить лише від деяких розрядів ключа. Це дозволяє спочатку відновити вказані розряди методом максимуму правдоподібності, а потім знайти решту ключа шляхом повного перебору. В [2] вказані способи вибору функцій F і g для побудови атаки, але не дано теоретичного обґрунтування ефективності таких способів. Крім того, залишається відкритим питання про можливість підвищити ефективність атаки, описаної в [2], шляхом вибору наближення функції F з більш широкого класу булевих функцій.

В статтях [9, 10] описана статистична атака на СПШ, що узагальнює атаку FKM, а також кубічну атаку. Вказана атака базується на наближенні булевих функцій алгебраїчно виродженими функціями [11], застосовуючи поліноміальний ймовірнісний алгоритм побудови (в певному сенсі як завгодно близьких до найкращих з можливих) наближень функції F за відомим допустимим для F підпростором.

Побудова наближень булевих функцій алгебраїчно виродженими функціями потребує ефективних алгоритмів побудови k-вимірних наближень булевих функцій [12] та алгоритмів перевірки k-вимірності булевих функцій [13].

У даній статті викладено результати дослідження k-вимірності булевої функції шифру LILI-128 з застосуванням вдосконаленого тесту розпізнавання k-вимірності булевих функцій, заданих за допомогою оракулів.

Основні означення та допоміжні результати

Наукові основи тесту викладені в [13]. Наведемо основні означення та допоміжні результати, що потрібні для викладення матеріалу даної роботи.

Нехай $f: V_n = \{0,1\}^n \to \{0,1\}$ – булева функція від n змінних, $\hat{f}(\alpha) = 2^{-n} \sum\limits_{x \in V_n} (-1)^{f(x) \oplus \alpha x}$, $\alpha \in V_n$ – її нормовані коефіцієнти Уолша-Адамара.

Функція $f: V_n = \{0,1\}^n \to \{0,1\}$ називається алгебраїчно виродженою, якщо вона є k-вимірною для деякого $k < n$ та невиродженою – в протилежному випадку [14 – 16].

Функція f називається k-вимірною, $k \in \overline{0, n-1}$, якщо множина $Sp(f) = \{\alpha \in V_n : \hat{f}(\alpha) \neq 0\}$ породжує підпростір вимірності не більше за k векторного простору V_n або, що рівносильно, якщо існує не менше за $n-k$ лінійно незалежних несуттєвих векторів функції f, тобто векторів, що належать множині $I_f = \{\alpha \in V_n : f(x \oplus \alpha) \equiv f(x), x \in V_n\}$ [17].

Відомо, що для помірних значень k функції, близькі до k-вимірних, володіють криптографічними слабкостями, що дозволяє здійснювати певні атаки на генератори гами, побудовані на основі зазначених функцій [18 – 20]. У зв'язку з цим практично важливою є розробка ефективних алгоритмів перевірки властивості k-вимірності булевих функцій.

Слід зауважити, якщо булева функція від n змінних f задана за допомогою вектора значень (таблиці істинності), то для перевірки умови приналежності булевої функції f до множини всіх k-вимірних булевих функцій n змінних можливо застосувати природній детермінований алгоритм, трудомісткість якого складає $O(n^2 2^n)$ двійкових операцій. Цей алгоритм полягає в обчисленні всіх значень $\hat{f}(\alpha)$ за допомогою швидкого перетворення Адамара [21, с. 217], побудові множини $Sp(f)$ та знаходженні базису векторного простору I_f методом Гауса. Функція f є k-вимірною в тому і тільки в тому випадку, коли отриманий базис містить не менше $n-k$ векторів. Цей алгоритм не застосовується на практиці, якщо n є достатньо великим числом (наприклад, $n \geq 64$), а функція f задається за допомогою оракула (певного алгоритму, що дозволяє обчислювати значення $f(x)$ за довільними вхідними аргументами $x \in V_n$).

В [17] запропоновано ймовірнісний алгоритм або тест k-вимірності, який для довільної функції $f: V_n \to \{0,1\}$, заданої за допомогою оракула, та чисел $k \in \overline{0, n-1}$, $\varepsilon \in (0,1)$ перевіряє основну гіпотезу H_0 про те, що f є k-вимірною функцією, проти альтернативи H_1: f знаходиться на відстані (Гемінга) не менше за $2^n \varepsilon$ від множини k-вимірних функцій n змінних. Зазначений алгоритм полягає в генерації незалежних випадкових рівноймовірних векторів $h_1, ..., h_l \in V_n$ та перевірці рівностей

$$f(h_j \oplus Z_{ij}) = f(Z_{ij}),\ i \in \overline{1,m} \tag{1}$$

для кожного $j \in \overline{1,l}$, де Z_{ij} – незалежні в сукупності випадкові рівноймовірні вектори з V_n, що не залежать від $h_1, ..., h_l$. Позначимо ν_l число значень $j \in \overline{1,l}$, для яких виконуються рівності (1). Тоді гіпотеза H_0 приймається, якщо $\frac{\nu_l}{l} \geq 0{,}9 \cdot 2^{-k}$ та відхиляється у протилежному випадку. В [17] пропонується вибрати $l = 2^k C$, $m = 2^k k \varepsilon^{-1} C'$, де $C, C' = const$, що приводить до оцінки трудомісткості алгоритму $O(2^{2k} k \varepsilon^{-1})$ запитів до оракула f (або $O(n 2^{2k} k \varepsilon^{-1})$ двійкових операцій).

Для оцінювання ймовірності помилки першого роду (тобто ймовірності того, що тест "не визнає" такою k-вимірну функцію) в [17] використовується нерівність Чернова:

$$\mathrm{P}\left(\frac{\nu_l}{l} < 0{,}9\cdot 2^{-k} \mid H_0\right) \le \mathrm{P}\left(\frac{\nu_l}{l} - \mathrm{E}\frac{\nu_l}{l} < -0{,}1\cdot 2^{-k} \mid H_0\right) \le \exp\left\{-0{,}02\cdot\frac{C}{2^k}\right\}. \qquad (2)$$

Зауважимо, що вираз у правій частині (2) залежить від k та не прямує до нуля, якщо k є (як завгодно повільно) зростаючою функцією від n, наприклад, $k = \lceil \log n \rceil$, $n \to \infty$.

Вдосконалений тест k-вимірності булевих функцій

В роботі [13] запропонований більш ефективний імовірнісний тест k-вимірності, трудомісткість якого складає $O(2^k k^2\, \varepsilon^{-1})$ запитів до оракула (або $O(n\, 2^k k^2\, \varepsilon^{-1})$ двійкових операцій). При цьому верхня межа ймовірності помилки першого роду запропонованого тесту не залежить від k, а верхня межа ймовірності помилки другого роду є по суті така ж сама, що й для тесту з [17].

Алгоритм перевірки k-вимірності булевих функцій, що запропонований в роботі [13], має такий вигляд.

Вхідні дані: $f : V_n \to \{0,1\}$, $k \in \overline{0, n-1}$, $\varepsilon \in (0,1)$.

Параметри: $t = k + c$, $m = 2^{t+4} t\, \varepsilon^{-1}\delta^{-1}$, де $c \in \mathrm{N}$, $\delta \in (0, 1/2)$, $c, \delta = const$).

1. Згенерувати випадкову рівноймовірну $t \times n$-матрицю X, побудувати множину $Sp(f_X)$, за якою знайти базис $a_1, ..., a_l$ векторного простору I_{f_X} (дуального до підпростору, що породжується множиною $Sp(f_X)$). Перевірити умову $l \ge t - k$, за виконанням якої перейти до кроку 2. У протилежному випадку – прийняти гіпотезу H_1 (f знаходиться на відстані не менше $2^n \varepsilon$ від множини k-вимірних функцій).

2. Для кожного $j \in \overline{1, l}$ покласти $h_j = a_j X$, згенерувати незалежні випадкові рівноймовірні вектори $Z_{1j}, ..., Z_{mj}$ та перевірити рівності (1). За виконанням зазначених рівностей для всіх $j \in \overline{1, l}$ прийняти гіпотезу H_0 (f – k-вимірна функція), у протилежному випадку – прийняти гіпотезу H_1.

Ймовірність помилки першого роду (відхилити вірну гіпотезу H_0) тесту, який реалізований описаним алгоритмом, не перевищує 2^{-c}, а ймовірність помилки другого роду (відхилити вірну гіпотезу H_1) не перевищує $\max\{5\cdot 2^{-c-1}, \delta + \exp\{-7c2^c\}\}$.

Потоковий шифр LILI-128

LILI-128 [22] – це синхронний потоковий шифр, що був учасником конкурсу NESSIE [23] та базується на регістрах зсуву з лінійним зворотнім зв'язком, з довжиною ключа, яка дорівнює 128 бітів. Генератор псевдовипадкових послідовностей LILI-128 використовує два регістри зсуву з лінійним зворотнім зв'язком та дві функції для генерації двійкової послідовності. Структура генератора представлена на рис. 1.

Як видно з рис. 1, в структурі генератору псевдовипадкових послідовностей шифру LILI-128 можливо виділити блок управління рухом та блок генерації даних. Вихідна послідовність $c(t)$ блоку управління рухом визначає закон руху блоку генерації даних.

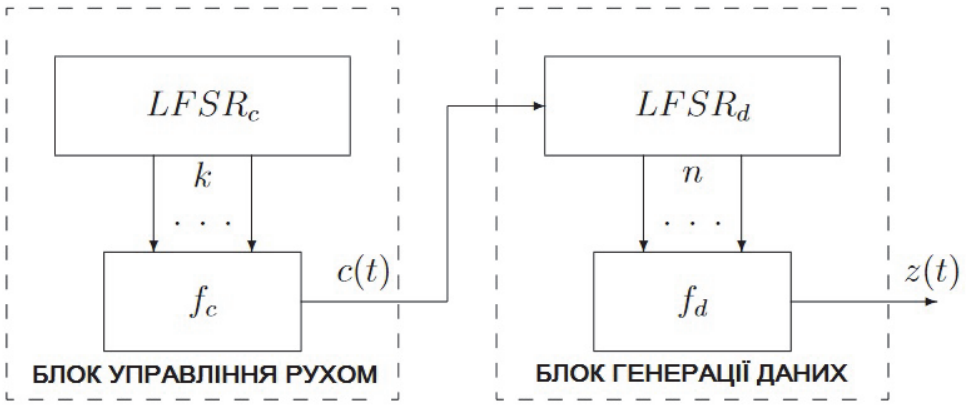

Рис. 1. Генератор LILI-128

Стан LILI-128 визначається як зміст двох регістрів зсуву з лінійним зворотнім зв'язком: $LFSR_c$ та $LFSR_d$, довжиною 39 та 89 біт відповідно. За поточним станом генератору обчислюються значення функцій f_c та f_d, а також функцій зворотного зв'язку. В якості оракулу була обрана булева функція від 89 змінних f_d.

Дослідження k-вимірності булевої функції шифру LILI-128

Обчислювальні експерименти проведені з використанням пакету прикладних програм Maple на ПЕОМ типу Intel(R) Core(TM) i7-3770K 3,5 GHz, 8 Gb RAM в середовищі операційної системи Windows 7 та були організовані наступним чином.

Фіксувалися значення вхідних даних k, ε та δ (від якого безпосередньо залежить ймовірність помилки другого роду та значення p_0 ймовірності помилки першого роду тесту, яке дозволяє обчислити значення параметрів $c = -\log_2(p_0)$ та $t = k + c$), що дозволяє обчислити значення $m = 2^{t+4} t\, \varepsilon^{-1}\delta^{-1}$. Під час проведення обчислювального експерименту значення ε, δ та p_0 були обрані рівними 0,125. Для кожного набору параметрів здійснювалося по 25 запусків тесту для кожного значення k від 1 до 10.

Таблиця 1

k	m	Кількість прийнятих гіпотез		Середній час перевірки гіпотези, сек.		$2^k k^2 \varepsilon^{-1}$
		H_0	H_1	H_0	H_1	
1	4	0	25	–	0,034	16
2	5	0	25	–	0,063	128
3	6	0	25	–	0,115	576
4	7	0	25	–	0,189	2048
5	8	0	25	–	0,301	6400
6	9	0	25	–	1,086	18432
7	10	0	25	–	2,116	50176
8	11	0	25	–	3,599	131072
9	12	3	22	70916,094	8,165	331776
10	13	25	0	152103,787	–	819200

Як видно з табл. 1, середній час перевірки гіпотези H_0 значно перевищує відповідний показник для H_1, що пов'язано з необхідністю виконання кроку 2 вдосконаленого тесту k-вимірності в повному обсязі для кожного $j \in \overline{1,l}$. Відзначимо також, що середній час пере-

вірки гіпотези залежить від k та зростає повільніше ніж аналітична оцінка трудомісткості алгоритму (кількість запитів до оракулу).

Висновки

В результаті виконання вдосконаленого тесту k-вимірності до функції f_d від 89 змінних шифру LILI-128 встановлено, що $k = 10$. Таким чином, $k < n$, що свідчить про потенційну можливість реалізації статистичної атаки, яка базується на наближенні булевих функцій алгебраїчно виродженими функціями.

Вдосконалений тест може бути застосований до аналізу відповідних властивостей булевих функцій (зокрема, від десятків чи сотен змінних), які використовуються в сучасних симетричних криптосистемах.

Список літератури:

1. Dinur I. Cube attacks on tweakable black box polynomials / I. Dinur, A. Shamir // Advances in Cryptology. – EUROCRYPT'09. Proceedings. Springer-Verlag, 2009. – P. 278–299.

2. Fischer S. Chosen IV statistical analysis for key recovery attacks on stream ciphers / S. Fischer, S. Khazaei, W. Meier // AFRICACRYPT 2008. Proceedings. Springer-Verlag, 2008. – P. 236–245.

3. Aumasson J.-Ph. Efficient FPGA implementations of high-dimensional cube testers on the stream cipher Grain-128 / J.-Ph. Aumasson, I. Dinur, L. Hensen, W. Meier, A. Shamir // Cryptology ePrint Archive. – URL: http://eprint.iacr.org/2009/218 (last access: 29.10.18).

4. Aumasson J.-Ph. Cube testers and key recovery attacks on reduced-raund MD6 and Trivium / J.-Ph. Aumasson, I. Dinur, W. Meier, A. Shamir // Fast Software Encryption – FSE'09. Proceedings. Springer-Verlag. 2009. – P. 1–22.

5. Aumasson J.-Ph. New features of latin dances: analysis of Salsa, ChaCha, and Rumba / J.-Ph. Aumasson, S. Fischer, S. Khazaei, W. Meier, C. Rechberger // Fast Softvare Encryption – FSE 2008, Proceedings. Springer-Verlag. 2008. – P. 470–488.

6. Dinur I. An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware / I. Dinur, T. Gueysu, C. Paar, A. Shamir, R. Zimmermann // Cryptology ePrint Archive. – URL: http://eprint.iacr.org/2011/282 (last access: 29.10.18).

7. Dinur I. Breaking Grain-128 with dynamic cube attacks / I. Dinur, A. Shamir // Fast Software Encryption – FSE'11. Proceedings. Springer-Verlag. 2011. – P. 167–187.

8. Faisal Sh. Extended cubes: enhancing cube attacks by low-degree non-linear equations / Sh. Faisal, M. Resa, W. Susilo, J. Seberry // Proc. of the 6-th ACM Symp. on Information, Comput. and Communication Security (AIACCS'11). 2011. – P. 296 – 305.

9. Алексейчук А.Н. Обобщенная статистическая атака на синхронные поточные шифры / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 3. – С. 54 – 65.

10. Алексейчук А.Н. Статистическая атака на генератор гаммы с линейным законом реинициализации начального состояния и функцией усложнения, близкой к алгебраически вырожденной / А.Н. Алексейчук, С.Н. Конюшок, А.Ю. Сторожук // Радиотехника. – 2014. – Вып. 176. – С. 13–21.

11. Алексейчук А.Н. Алгебраически вырожденные приближения булевых функций / А.Н. Алексейчук, С.Н. Конюшок // Кибернетика и системный анализ. – 2014. – Т. 50. – № 6. – С. 3–14.

12. Олексійчук А.М. Швидкі алгоритми побудови k-вимірних наближень наближень булевих функцій / А.М. Олексійчук, С.М. Конюшок, А.Ю. Сторожук // Захист інформації. – 2015. – Т. 17. – № 1. – С. 43–52.

13. Алексейчук А.Н. Усовершенствованный тест k-мерности для булевых функций / А.Н. Алексейчук, С.Н. Конюшок // Кибернетика и системный анализ. – 2013. – Т. 49. – № 2. – С. 27 – 35.

14. Lechner, R. L. Harmonic analysis of switching functions / R.L. Lechner // Recent Developments in Switching Theory. – New-York. Academic Press, 1971. – P. 122–228.

15. Dawson E. Construction of correlation immune Boolean functions / E. Dawson, C.K. Wu // Information and Communication Security, Proceedings. Berlin. Springer-Verlag, 1997. – P. 170–180.

16. Алексеев, Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. – 2011. – № 2(12). – С. 5–16.

17. Gopalan P. Testing Fourier dimensionality and sparsity / P. Gopalan, R. O'Donnell, A. Servedio, A. Shpilka, K. Wimmer // SIAM J. on Computing. – 2011. – Vol. 40(4). – P. 1075 – 1100.

18. Golic J., Morgari G. On the resynchronization attack // Fast Software Encryption. – FSE'03, Proceedings. – Springer-Verlag, 2003. – P. 100 – 110.

19. Алексеев Е.К. О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. – 2011. – № 2(12). – С. 5 – 16.

20. Алексеев Е.К. Об атаке на фильтрующий генератор с функцией усложнения, близкой к алгебраически вырожденной // Материалы Шестой междунар. науч. конф. по проблемам безопасности и противодействия терроризму, 11 – 12 ноября 2010 г., Том 2. – Москва : МЦНМО, 2011. – С. 114 – 122.

21. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – Москва : МЦНМО, 2004. – 470 с.

22. Simpson L.R. LILI Keystream Generator / L.R. Simpson, E. Dawson, J.D. Golić, W.L. Millan // Selected Areas in Cryptography. – SAC 2000. Lecture Notes in Computer Science, vol 2012. – Springer, Berlin, Heidelberg. – P. 248 – 261.

23. NESSIE New European Schemes for Signatures, Integrity, and Encryption // URL: https://www.cosic.esat.kuleuven.be/nessie/ (last access: 29.10.18).

Інститут спеціального зв'язку та захисту інформації
національного технічного університету України
«Київський політехнічний інститут» імені Ігоря Сікорського

Надійшла до редколегії 01.11.2018