УДК 004.056.55

СПОСОБИ ЗМЕНШЕННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ ШИФРУ ШЛЯХОМ ЗАМІНИ ЙОГО ОКРЕМИХ КОМПОНЕНТ ПІД ВИДОМ ЗБІЛЬШЕННЯ СТІЙКОСТІ

О. Ю. Галій[1, a]

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

Анотація

В роботі наведено основні шляхи зменшення криптографічної стійкості до різницевого криптоаналізу шляхом заміни деяких операцій в ключовому суматорі, а саме операцію модульного додавання замінено на операцію покомпонентного додавання та навпаки.

Ключові слова: диференціальний криптоаналіз, диференціальна імовірність, симетрична криптографія, покомпонентне додавання, модульне додавання, блочний шифр.

Вступ

Диференціальний криптоаналіз був запропонований в 1991 році Біхамом і Шаміром [1] і є потужним механізмом криптоаналізу блочних шифрів.

Одним з обов'язкових критеріїв сучасних блочних шифрів є стійкість до різницевого криптоаналізу. Варто зазначити, що традиційний підхід до побудови сучасних блокових шифрів ґрунтується на загальноприйнятих принципах – розсіюванні та перемішуванні, сформульованих ще у фундаментальній роботі К. Шеннона [2]. Під розсіюванням мається на увазі вплив одного знаку відкритого тексту на багато знаків шифрованого тексту, що дозволяє «згладити» статистичні властивості відкритих повідомлень.

При побудові шифрів намагаються досягти якнайкращого розсіювання статистичних залежностей, використовуючи для цього прості перетворення, котрі можна легко реалізувати на сучасних ЕОМ. Проте, коли автори намагаються оцінювати блочні шифри за допомогою методів криптоаналізу різних типів, зокрема різницевого криптоаналізу, вони здебільшого використовують його спрощені модифікації, а саме – можуть замінювати модульне додавання у ключовому суматорі на покомпонентне (побітове). Такі спрощення найчастіше використовувалися для алгоритмів ГОСТ 28147-89, "Мухомор", "Калина" [3, 4]. Замість операції побітового додавання використовувалася операція додавання за модулем 2^{32} [5].

Метою даної роботи є зменшення криптографічної стійкості шляхом заміни його окремих компонент, а саме заміна ключового суматора з операції побітового додавання на операцію модульного додавання і навпаки.

[a] olexander.halii@gmail.com

1. Загальні відомості

Нехай $\alpha, \beta \in V_q \to V_q$ – бієктивна функція, $k \in K$-ключовий простір. Диференціал булевої функції f – пара двійкових векторів (α, β) така, що виконується співвідношення $f(z \oplus \alpha) \oplus f(z) = \beta$. Імовірність диференціалу (α, β) функції f величина

$$d^f_{\oplus,\oplus}(\alpha, \beta) = \frac{1}{2^q} \sum_{z \in V_q} [f(z \oplus \alpha) \oplus f(z) = \beta],$$

де [твердження] – дужки Айверсона [6]. Середня за ключами імовірність диференціалу (α, β) функції f_k в точці z визначається за формулою

$$d^{f_k}_{\oplus,\oplus} = \frac{1}{|K|} \sum_{k \in K} [f(z \oplus \alpha] \oplus f(z) = \beta],$$

де $k \in V_m, f_k : V_q \times V_m \to V_m$. Для довільного $n \in N$ позначимо через $V_n = \{0, 1\}^n$ множину n-вимірних бітових векторів. Тут і надалі з вектором V_n будемо ставити у відповідність цілі числа від 0 до 2^{n-1}. Через $\alpha \oplus \beta$ будемо позначати результат побітового додавання векторів α та β, а через $\alpha + \beta$ операції додавання та віднімання цілих чисел за модулем 2^{32}. Бієктивне відображення $S : V_n \to V_n$ задамо наступним чином: $\forall x \in V_n : S(x) = (S^{(p)}, ..., S^{(1)}(x^{(1)})), x^{(i)} \in V_u, i = \overline{1, p}$ де $S^{(i)} : V_u \to V_u, i = \overline{1, p}$. Це відображення також називають блоком підстановки, а відображення $S^{(i)}$-S-блоками.

2. Заміна ключового суматора з операції побітового додавання на операцію модульного додавання.

Ми будемо розглядати раундові функці,ї котрі мають вигляд $F_k(x) = L(S(x \oplus k))$, або $F_k(x) = L(S(x + k))$. Для довільного S блоку покладемо

1) $d^s_{\oplus,+} = 2^{-u} \sum_{k \in V_u} \delta(s(k \oplus \alpha) - s(k), \beta)$
2) $d^s_{\oplus,\oplus} = 2^{-u} \sum_{k \in V_u} \delta(s(k \oplus \alpha) \oplus s(k), \beta)$
3) $d^s_{+,+} = 2^{-u} \sum_{k \in V_u} \delta(s(k + \alpha) - s(k), \beta)$

Табл. 1. Приклад s-блоків, що задовільняють умові $\triangle^s_{+,\oplus} > \triangle^s_{\oplus,\oplus}$

s-блок	$\triangle^s_{+,\oplus}$	$\triangle^s_{\oplus,\oplus}$
s1	0,042	0,0390
s2	0,042	0,0390
s3	0,042	0,0390
s4	0,042	0,0390
s5	0,042	0,0390
s6	0,042	0,0390
s7	0,042	0,0390
s8	0,042	0,0390
s9	0,042	0,0390
s10	0,042	0,0390
s11	0,042	0,0390
s12	0,042	0,0390

Табл. 2. Приклад s-блоків, що задовільняють умові $\triangle^s_{\oplus,\oplus} > \triangle^s_{+,\oplus}$

s-блок	$\triangle^s_{\oplus,\oplus}$	$\triangle^s_{+,\oplus}$
$s1$	0,4687	0,03125
$s2$	0,4687	0,03125
$s3$	0,3906	0,03125
$s4$	0,3906	0,03125
$s5$	0,4687	0,03125
$s6$	0,4687	0,0273
$s7$	0,4687	0,0273
$s8$	0,4687	0,0273
$s9$	0,4687	0,0273
$s10$	0,4687	0,03125
$s11$	0,4687	0,03125
$s12$	0,4687	0,0234

4) $d^s_{+,\oplus} = 2^{-u} \sum_{k \in V_u} \delta(s(k+\alpha) \oplus s(k), \beta)$

Також покладемо $\triangle^s_{\oplus,+} = maxd^s_{\oplus,+}$, де $\alpha, \beta \in V_u \setminus \{0\}$ і аналогічно визначимо $\triangle^s_{\oplus,\oplus}$, $\triangle^s_{+,+}$ та $\triangle^s_{+,\oplus}$.

Заміна операції побітого додавання на операцію модульного додавання збільшить нелінійсть шифру, що в свою чергу призведе до збільшення стійкості до різницевого криптоаналізу, проте у раундових функціях наявні такі S-блоки, для яких виконується наступне $\triangle^s_{+,\oplus} > \triangle^s_{\oplus,\oplus}$, тобто при виборі таких S-блоків ми понизимо стійкість шифру до різницевого криптоаналізу. Збільшуючи імовірність раундового диференціалу, ми збільшуємо імовірність диференціалу та диференціальної характеристики всього шифру, тим самим зменшуючи його стійкість до різницевого криптоаналізу. Зменшення стійкості шифру можна досягти заміною ключового суматора. Заміна ключового суматора з операції побітового додавання на операцію модульного додавання призведе до зменшення стійкості до цілочисельного або класичного різницевого криптоаналізу.

Після такої заміни максимальна імовірність раундового побітового диференціалу буде визначатись параметром $\triangle^s_{+,\oplus}$ замість $\triangle^s_{\oplus,\oplus}$, а імовірність раундового цілочисельного диференціалу – параметром $\triangle^s_{+,+}$ замість $\triangle^s_{\oplus,+}$.

3. Заміна ключового суматора з операції модульного додавання на операцію побітового додавання

Для збільшення швидкодії шифру можна замінити операцію модульного додавання на операцію побітового додавання, так як S-блоки забезпечують достатню нелінійність, тому внесення додаткової нелінійності є зайвим, до того ж суттєво вповільнює процес шифрування. Проте аналогічно другому розділу у раундовій функції наявні такі S-блоки, для яких виконується наступне: $\triangle^s_{\oplus,\oplus} > \triangle^s_{+,\oplus}$ або $\triangle^s_{\oplus,+} > \triangle^s_{+,+}$. Отже наявність таких блоків значно зменшить стійкість до різницевого криптоаналізу.

Висновки

Результати експериментального дослідження, котрі наведені в цій роботі, показали, що існують можливі атаки на пониження стійкості до диференціального криптоаналізу. Криптоаналітик, використовуючи сучасну обчислювальну техніку та алгоритми, зможе штучно понизити стійкість шляхом заміни деяких операцій в S-блоках.

Перелік використаних джерел

1. Biham E,Shamir A. Differential cryptanalysis of DES-like cryptosystems — // Journal of Cryptology, 1991- V. 4. – № 1. – P. 3. — 72
2. Шеннон К. Теория связи в секретных системах //Работы по теории информации и кибернетике. — М. : Издательство иностранной литературы, 1963. — 333-402 с.
3. Горбенко І. Д.,Бондаренко М. Ф. Перспективний блоковий шифр «Мухомор» – основні положення та специфікація // Прикладна радіоелектроніка. — Харківський національний університет радіоелектроніки, 2007.- т.6, №2. — 147-157 с.
4. Горбенко І. Д.,Тоцький О. С.,Казьміна С. В. Перспективний блоковий шифр «Калина» – основні положення та специфікація // Прикладна радіоелектроніка. — Харківський національний університет радіоелектроніки, 2007.- т.6, №2. — 195-208 с.
5. Галинский В. А.Вероятностные свойства переносов при сложении по модулю 2^n // Обозрение прикладной и промышленной математики. — 2003.Т.10, вып.1. — 129-130 с.
6. Яковлєв С. В.Доказова та практична стійкість R-схеми блочного шифрування до диференціального криптоаналізу // Вісник Національного університету "Львівська політехніка секція "Комп'ютерні науки №744— Львів,2013 — 107-11 с.