УДК 004.056.55:512.6+519.248

ДОСЛІДЖЕННЯ РОЗПОДІЛІВ КОЕФІЦІЄНТІВ БУМЕРАНГОВОЇ ЗВ'ЯЗНОСТІ ДЛЯ РІЗНИХ АЛГЕБРАЇЧНИХ ОПЕРАЦІЙ

М. М. Шашенок[1,a]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі досліджуються алгебраїчні та статистичні властивості коефіцієнтів бумерангової зв'язності (BCT) відносно різних алгебраїчних операцій. Введено поняття гібридного коефіцієнту бумерангової зв'язності, який визначається використанням різних алгебраїчних операцій для обчислення різниць на вході та на виході перетворення; сформульовано основні алгебраїчні властивості таких коефіцієнтів. Для звичайних та гібридних коефіцієнтів BCT було експериментально перевірено припущення про їх належність розподілу Пуассона та оцінено параметри розподілу. Виявилось, що для різниць порядку 2 розподіл BCT описується розподілом Пуассона з параметром 1, а для усіх інших різниць — розподілом Пуассона із параметром 2.

Ключові слова: диференціальний криптоаналіз, атака бумерангів, коефіцієнт бумерангової зв'язності, BCT

Вступ

Розвиток диференціального криптоаналізу призвів до винайдення багатьох форм криптоаналітичних атак на різноманітні симетричні криптосистеми. Одним з таких методів аналізу стала «атака бумерангів», вперше запропонована Д. Вагнером у роботі [1] і в подальшому розвинена та вдосконалена у серії робіт, зокрема, [2, 3, 4]. На відміну від класичної схеми диференціального криптоаналізу, який досліджував пари відкритих текстів із відомими різницями та відповідних їм шифротекстів, новий метод оперує впорядкованими четвірками відкритих текстів та шифротекстів із відомими залежностями. Стійкість до атак бумерангів визначається спеціальними параметрами, які одержали назву *коефіцієнти бумерангової зв'язності*. Відповідно, розподіл значень даних коефіцієнтів є важливим як для аналізу існуючих криптосистем, так і для побудови нових шифрів із гарантованою стійкістю до атак бумерангів.

В опублікованих джерелах зазвичай розглядаються диференціали та бумеранги, побудовані на основі побітового додавання. Цей підхід зазвичай не дозволяє аналізувати недвійкові шифри або шифри, які використовують декілька алгебраїчних операцій у своїй будові. У роботі [5] було введено поняття коефіцієнту бумерангової зв'язності відносно операції модульного додавання та досліджено його алгебраїчні властивості. У даній роботі буде введено та досліджено гібридні коефіцієнти бумерангової зв'язності по відношенню до різних алгебраїчних операцій (зокрема, побітового та модульного додавання) та сформульовано їх основні алгебраїчні властивості. Для усіх видів коефіцієнтів буде статистично перевірена гіпотеза про те, що їх розподіли на випадкових бієктивних відображеннях відповідають розподілам Пуассона, та будуть емпірично знайдені параметри даних розподілів.

1. Атака бумерангів та коефіцієнти бумерангової зв'язності

Атаки бумерангів на шифруюче перетворення E розглядають четвірки вхідних текстів та відповідних їм шифротекстів: $C_i = E(P_i)$, $i = \overline{1,4}$, які пов'язані співвідношеннями $P_1 \oplus P_2 = \alpha$, $C_1 \oplus C_3 = \beta$, $C_2 \oplus C_4 = \beta$ для деяких заздалегідь визначених векторів α, β. Якщо при виконанні заданих умов подія $P_3 \oplus P_4 = \alpha$ виконується з великою імовірністю, це дозволяє ефективно розрізнити шифр E від випадкової перестановки. Відповідно, для проведення криптоаналізу необхідно дослідити рівняння

відносно $x \in_R V_n$. Дане рівняння будемо називати *рівнянням бумерангової зв'язності* перетворення E. Для кожної пари різниць (α, β) ймовірність виконання даного рівняння при випадково обраному значенні x описує складність проведення самої атаки: чим більша імовірність, тим ефективніша атака.

Формальний параметр, який описує стійкість атак бумерангів, можна визначити у такий спосіб [2]. Нехай $F\colon V_n \to V_n$ — бієктивне відображення; тоді для заданої пари двійкових векторів-різниць (α, β) та операції побітового додавання $\oplus$ *коефіцієнт бумерангової зв'язності* $BCT^F_\oplus(\alpha, \beta)$ (від англ. «*Boomerang Connectivity Table*») визначається таким чином:

$$BCT^F_\oplus(\alpha,\beta) = |\{x \in V_n\colon F^{-1}(F(x) \oplus \beta) \oplus \\ \oplus F^{-1}(F(x \oplus \alpha) \oplus \beta) = \alpha\}|.$$

Як випливає з означення, введена величина ви-

[a] brunoquinttone@gmail.com

значає кількість двійкових векторів з лінійного простору V_n, які задовільняють рівнянню бумерангової зв'язності. Даний параметр був досліджений у роботах [2, 3, 4]; зокрема, були знайдені точні вирази для розподілу цієї величини та встановлено, що її можна апроксимувати законом розподілу Пуассона.

Як альтернативу, для недвійкових шифрів було запропоновано розглядати коефіцієнти бумерангової зв'язності з іншими операціями — наприклад, з операцією додавання за модулем 2^n [5]. У такому випадку коефіцієнт бумерангової зв'язності визначатиметься як

$$BCT_{+}^{F}(\alpha,\beta) = |\{x \in V_n \colon F^{-1}(F(x)+\beta) = \\ = F^{-1}(F(x+\alpha)+\beta)+\alpha\}|.$$

Зауважимо, що в опублікованих джерелах не розглядались гібридні випадки, коли для різниць на вході та на виході відображення використовуються різні алгебраїчні операції. Введемо за аналогією поняття *гібридних коефіцієнтів бумерангової зв'язності*: для бієктивного відображення F, операцій побітового $\oplus$ та модульного $+$ додавань і пар векторів-різниць (α,β) визначимо величини

$$BCT_{+,\oplus}^{F}(\alpha,\beta) = |\{x \in V_n \colon F^{-1}(F(x+\alpha)\oplus\beta) = \\ = \alpha + F^{-1}(F(x)\oplus\beta)\}|;$$
$$BCT_{\oplus,+}^{F}(\alpha,\beta) = |\{x \in V_n \colon F^{-1}(F(x\oplus\alpha)+\beta) = \\ = \alpha \oplus F^{-1}(F(x)+\beta)\}|.$$

Далі ми дослідимо алгебраїчні та статистичні властивості уведених гібридних коефіцієнтів та їх порівняння зі звичайними коефіцієнтами бумерангової зв'язності.

2. Алгебраїчні властивості гібридних коефіцієнтів бумерангової зв'язності

Гібридні коефіцієнти бумерангової зв'язності, як було виявлено, зберігають більшу частину властивостей звичайних коефіцієнтів. Перелічимо основні з них; тут і далі α та β є довільними двійковими векторами.

1. Якщо одна з різниць є нульовою, то коефіцієнти бумерангової зв'язності сягають максимально можливого значення:
$$BCT_{+,\oplus}^{F}(0,\beta) = BCT_{+,\oplus}^{F}(\alpha,0) = 2^n,$$
$$BCT_{\oplus,+}^{F}(0,\beta) = BCT_{\oplus,+}^{F}(\alpha,0) = 2^n.$$
2. $BCT_{+,\oplus}^{F^{-1}}(\alpha,\beta) = BCT_{\oplus,+}^{F}(\beta,\alpha)$.
3. Усі значення $BCT_{+,\oplus}^{F}(\alpha,\beta)$ та $BCT_{\oplus,+}^{F}(\alpha,\beta)$ є парними числами.
4. Нехай $\lambda\colon V_n \to V_n$, $\mu\colon \mathbb{Z}_{2^n} \to \colon \mathbb{Z}_{2^n}$ — невироджені афінні перетворення над відповідними структурами, і $G(x) = \lambda(F(\mu(x)))$, $H(x) = \mu(F(\lambda(x)))$; тоді
$$BCT_{+,\oplus}^{G}(\alpha,\beta) = BCT_{+,\oplus}^{F}(\mu(\alpha),\lambda^{-1}(\beta)),$$
$$BCT_{\oplus,+}^{H}(\alpha,\beta) = BCT_{\oplus,+}^{F}(\lambda(\alpha),\mu^{-1}(\beta)).$$

Те, що алгебраїчні властивості (в основному) збігаються підводить до думки, що і статистичні особливості теж будуть якщо і не ідентичними, то майже напевно доволі схожими, матимуть спільні риси, що може допомогти зрозуміти як себе поводить ця статистика.

3. Статистичні властивості

Постановка задачі

Статистичні властивості криптографічних параметрів описуються їх розподілами при випадковому виборі досліджуваного перетворення (S-блоку чи шифру). У даному розділі ми будемо досліджувати розподіли гібридних коефіцієнтів бумерангової зв'язності по відношенню до операцій побітового та модульного додавання, а також розподіл звичайних коефіцієнтів бумерангової зв'язності по відношенню до модульного додавання.

Скористаймося наступним припущенням: всі значення усіх варіантів гібридних BCT — вибірка з розподілу Пуассона. Ця гіпотеза спадає першою на думку, якщо згенерувати багато випадкових бієкцій F, порахувати відповідні функції для заданих векторів α та β і побудувати діаграми, бо отримані графіки будуть дуже схожі до рисунків вибірок з розподілу Пуассона.

Окрім цього, необхідно зауважити, що між коефіцієнтами бумерангової зв'язності та імовірностями диференціалів перетворення існує тісний зв'язок, а імовірності диференціалів також асимптотично описуються розподілами Пуассона [6].

Саме тому ми поставимо задачу у такий спосіб: *для заданих α, β оцінити параметри $\theta_1, \theta_2, \theta_3$, де*

$$\begin{aligned} BCT_{+}^{F}(\alpha,\beta) &\sim Poisson(\theta_1),\\ BCT_{+,\oplus}^{F}(\alpha,\beta) &\sim Poisson(\theta_2),\\ BCT_{\oplus,+}^{F}(\alpha,\beta) &\sim Poisson(\theta_3), \end{aligned}$$

при випадковому рівномірному виборі відображення F з множини усіх бієктивних відображень над V_n.

Проведення та аналіз результатів експерименту

Для проведення статистичного експерименту для пари різниць (α,β) генерувалась вибірка з 10^5 випадкових перестановок, на основі яких обчислювалось значення коефіцієнтів бумерангової зв'язності; для випадкової генерації використовувались вбудовані методі пакету Numpy у мові програмування Python. Потрібно зазначити, що для кожної такої пари різниць BCT матиме власний вибірковий розподіл, але, незважаючи на це, були встановлені загальні закономірності. В експериментах розглядались перетворення розміру $n = 8$, оскільки воно є типовим для сучасних S-блоків і достатньо великим для дослідження поведінки коефіцієнтів BCT.

Спершу було реалізовано тест Колмогорова-Смирнова для встановлення, чи належать згенеровані вибірки значень гібридних коефіцієнтів BCT до розподілу Пуассона. Було обрано рівень значущості

0.95, якому відповідає критичне значення ≈ 0.006198. Значення тестової статистики для $BCT_{+,\oplus}$, встановлене експериментально, дорівнювало $6.23 \cdot 10^{-11}$, а для $BCT_{\oplus,+}$ — $(3.51 \cdot 10^{-13})$; обидва значення не перевищують відповідного критичного значення. Таким чином, дана статистична гіпотеза підтверджується і вибірковий розподіл відповідає розподілу Пуассона. Необхідно зауважити, що експериментально одержані вибіркові розподіли для звичайних коефіцієнтів $BCT_{\oplus}$ та BCT_{+} також проходять відповідні тести на належність до розподілу Пуассона: значення тестової статистики для $BCT_{\oplus}$ виявилось $4.42 \cdot 10^{-17}$, а для BCT_{+} — $1.2 \cdot 10^{-6}$, що також не перевищує критичне значення 0.006198.

Отже, подальша задача сформулювалась як побудова оцінки для параметрів відповідних апроксимуючих розподілів Пуассона, яку ми проводили за допомогою метода максимальної правдоподібності. Як відомо, оцінка для величини з розподілу Пуассона у такому випадку будується як середнє вибіркове: $\theta_i = \overline{X}$, де X — згенерована вибірка значень. Інші способи побудови оцінки параметрів (метод Монте-Карло, баєсове оцінювання) на практиці дають гірше наближення для розподілу Пуассона.

Експерименти дали такі результати: для будь-якого $i = \overline{1,3}$ параметри розподілів оцінюються як

$$\theta_i = 1, \qquad \operatorname{ord}\alpha \neq 2 \text{ або } \operatorname{ord}\beta \neq 2;$$
$$\theta_i = 2, \qquad \operatorname{ord}\alpha = \operatorname{ord}\beta = 2.$$

Приклади гістограм, які ілюструють розподіли звичайних та гібридних коефіцієнтів бумерангової зв'язності, наведено на рис. 1–6.

Окремо був проведений тест χ^2 для перевірки того, чи співпадають в наших величин дисперсії та математичні сподівання. Результати експериментів відповідають даній гіпотезі. У даному випадку критичне значення дорівнює ≈ 1.9594, а значення тестової статистики для коефіцієнтів BCT_{+} виявилось ≈ 1.0141, що менше критичного значення; для інших коефіцієнтів бумерангової зв'язності одержано аналогічні результати. Відповідно, можна прийняти таку гіпотезу:

$$\forall \alpha, \beta \in V_n : \mathbb{E}[BCT^F(\alpha,\beta)] = \operatorname{Var}[BCT^F(\alpha,\beta)]$$

для усіх типів коефіцієнтів BCT. Цей момент є важливим, оскільки саме для пуассонівських розподілів характерною рисою є співпадіння математичного сподівання та дисперсії. Звичайно, виключно з цього не можна одразу робити висновок щодо виду розподілу, оскільки існує нескінченна кількість інших випадкових величин, для яких справедливо таке твердження, але це є ще одним аргументом на користь того, що початкове припущення про апроксимацію розподілів коефіцієнтів бумерангової зв'язності розподілами Пуассона є правильним. Відмітимо також, що якщо побудувати 0.95-довірчий інтервал для значень досліджуваних статистик, то більша частина значень буде належати множині $\{0, 2, 4, 6\}$, яка відповідає довірчому інтервалу розподілів Пуассона із знайденими параметрами. Ці міркування також

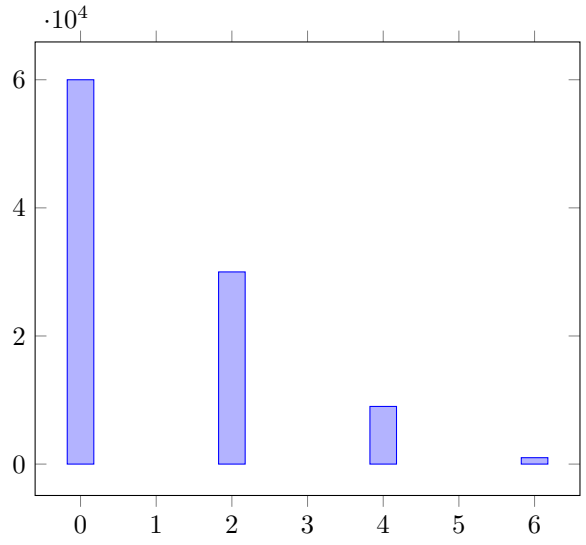

Рис. 1. Приклад розподілу $BCT_{+,\oplus}(\alpha,\beta)$ при $\operatorname{ord}\alpha \neq 2$.

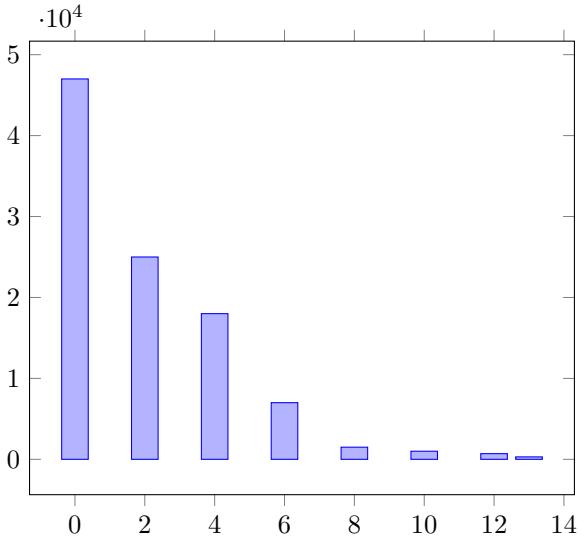

Рис. 2. Приклад розподілу $BCT_{+,\oplus}(\alpha,\beta)$ при $\operatorname{ord}\alpha = 2$.

підтверджуються емпірично, що ілюструється наведеними гістограмами.

Висновки

У даній роботі було розглянуто коефіцієнти бумерангової зв'язності криптографічних перетворень із використанням різних алгебраїчних операцій для обчислення вхідних та вихідних різниць між текстами. Для таких гібридних коефіцієнтів було сформульовано основні алгебраїчні властивості, які в цілому виявились аналогічними властивостям звичайних коефіцієнтів. Було проведено ряд статистичних експериментів, які показали, що розподіл усіх типів коефіцієнтів бумерангової зв'язності відповідає розподілу Пуассона, параметр якого дорівнює 1 або 2, що визначається порядками відповідних різниць.

Слід зауважити, що точні розподіли величин, які

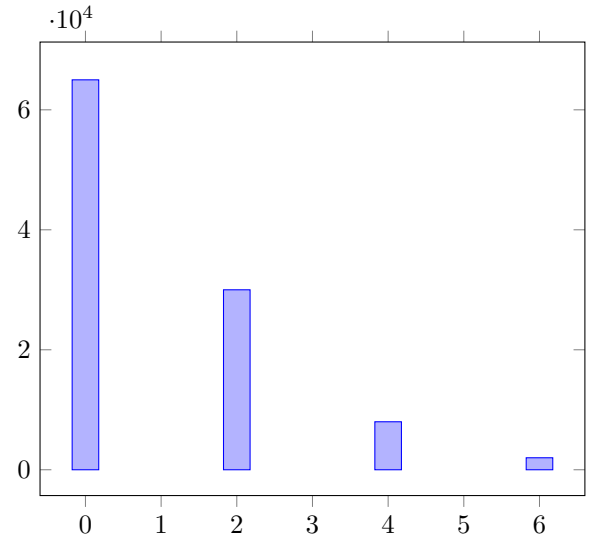

Рис. 3. Приклад розподілу $BCT_{\oplus,+}(\alpha,\beta)$ при $\operatorname{ord}\beta \neq 2$.

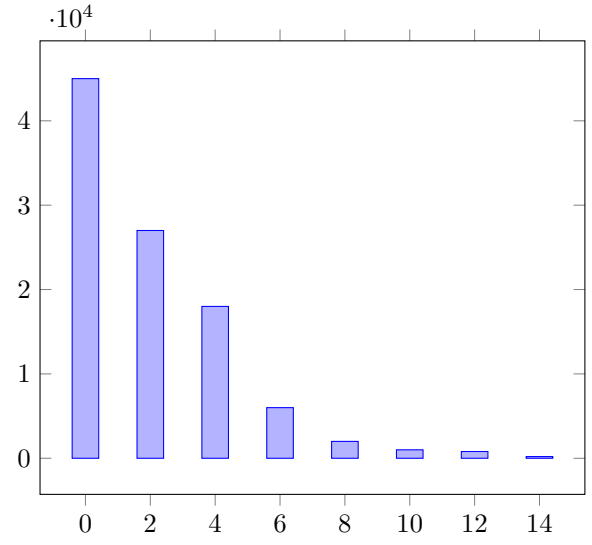

Рис. 4. Приклад розподілу $BCT_{\oplus,+}(\alpha,\beta)$ при $\operatorname{ord}\beta = 2$.

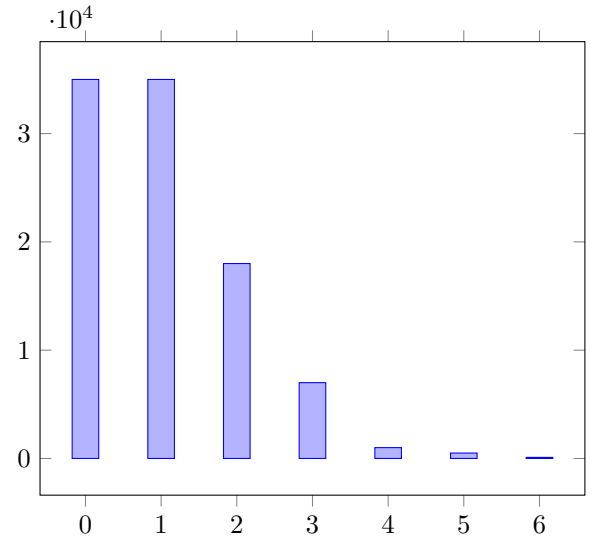

Рис. 5. Приклад розподілу $BCT_{+}(\alpha,\beta)$ при $\operatorname{ord}\alpha \neq 2$, $\operatorname{ord}\beta \neq 2$.

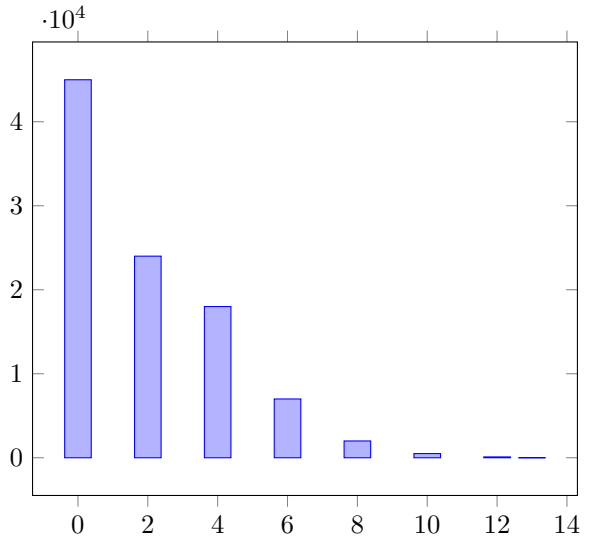

Рис. 6. Приклад розподілу $BCT_{+}(\alpha,\beta)$ при $\operatorname{ord}\alpha = 2$, $\operatorname{ord}\beta = 2$.

розглядаються, невідомі, а їх одержання є нетривіальною математичною задачею. Знання точних розподілів може допомогти оцінювати стійкість до атак бумерангів для перетворень (зокрема, S-блоків) малого розміру.

Перелік використаних джерел

1. *Wagner D.* The Boomerang Attack // Fast Software Encryption. — Springer Berlin Heidelberg, 1999. — С. 156—170. — ISBN 978-3-540-48519-3.
2. Boomerang Connectivity Table: A New Cryptanalysis Tool / C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song. — 2018. — URL: https://eprint.iacr.org/2018/161. Cryptology ePrint Archive, Paper 2018/161.
3. *Nyberg K.* The Extended Autocorrelation and Boomerang Tables and Links Between Nonlinearity Properties of Vectorial Boolean Functions. — 2019. — URL: https://eprint.iacr.org/2019/1381. Cryptology ePrint Archive, Paper 2019/1381.
4. *Tian S., Boura C., Perrin L.* Boomerang Uniformity of Popular S-box Constructions. — 2019. — URL: https://eprint.iacr.org/2019/1002. Cryptology ePrint Archive, Paper 2019/1002.
5. *Власенко Н. М., Яковлєв С. В.* Алгебраїчні властивості коефіцієнтів бумерангової зв'язності відносно додавання за модулем // Теоретичні і прикладні проблеми фізики, математики та інформатики (15 червня 2022 р., м. Київ, Україна). — Київ : КПІ ім. Ігоря Сікорського, видавництво «Політехніка», 2022. — С. 216—218.
6. *Hawkes P., O'Connor L.* XOR and Non-XOR Differential Probabilities // Advances in Cryptology - EUROCRYPT '99. Т. 1592. — Springer, 1999. — С. 272—285. — (Lecture Notes in Computer Science). — DOI: 10.1007/3-540-48910-X_19.