УДК 004.056.55

ПОРІВНЯЛЬНИЙ АНАЛІЗ КРИПТОГРАФІЧНИХ ВЛАСТИВОСТЕЙ БЛОКІВ ПІДСТАНОВКИ ДЕЯКИХ СУЧАСНИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ

О. В. Науменко[1, a]

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

Анотація

Проаналізовано різні криптографічні властивості блоку підстановки для деяких алгоритмів, які є сучасними стандартами блокового шифрування. Показано, що ці властивості не є однаковими для всіх цих алгоритмів. Також показано, що деякі з властивостей є інваріантними відносно різних перетворень.

Ключові слова: блоковий шифр, блок підстановки, стандарт блокового симетричного шифрування

Вступ

Ми живемо в світі, в якому з кожним днем, або навіть з кожною хвилиною відбуваються зміни в розвитку інформаційних технологій, тому, навіть якщо питання конфіденційності інформації, цілісності даних та стійкості алгоритмів шифрування завжди займало провідне місце в задачах криптографії, зараз воно постає ще гострішим.

На даний момент розробкою стійких блокових симетричних шифрів (БСШ) займаються науковці кожної країни світу, тому що інформаційно-телекомунікаційні системи потребують послуг, що спрямовані саме на захист інформації, збереження її цілісності, доступності та конфіденційності. Не менш важливими факторами є швидкодія БСШ та зрозумілість реалізації, захищеність від відомих атак. За останні роки розвиток криптографії пришвидшився, зокрема в Україні та країнах СНД було прийнято нові національні стандарти (НС) симетричного шифрування. В Білорусі в 2011 році в якості державного стандарту був прийнятий блоковий шифр (БШ) «BelT»[1], в Україні з 2014 року місце НС зайняв шифр «Калина»[2], в Росії з 2015 року діє БШ «Кузнєчік»[3]. Також цікавим є шифр «Present»[4], який в 2012 році було включено в стандарт міжнародного шифрування організаціями ISO та IEC. Вищезгадані шифри використовують алгоритми шифрування, що відповідають принципам Шенона щодо перемішування (confusion) та розсіювання (diffusion)[5], які застосовують багаторазово та послідовно для того, щоб забезпечити високий рівень криптографічної стійкості. Нелінійною операцією для перемішування є таблиці підстановки, або S-блоки, якість яких повинна бути високою задля забезпечення стійкості всього шифруючого перетворення та унеможливлення крипто аналітичних атак. Тому дослідження властивостей обраних s-блоків є однією з найважливіших задач сучасної криптографії.

1. Необхідні терміни та позначення

Нехай n, p, t – натуральні числа, $n = pt$. Позначимо $V_n = \{0,1\}^n$ множину n-вимірних бітових векторів, а знаком $\oplus$ будемо позначати операцію побітового додавання (XOR) на цій множині.

Кожен елемент $x \in V_n$ будемо позначати як $x = (x_n, \dots, x_1)$, $x_i \in \{0,1\}$, $i = \overline{1,n}$. Також для подальшого викладення нам потрібне позначення $x = (x^{(i)}, \dots x^{(1)})$, де $x^{(i)} \in V_t$, $i = \overline{1,p}$; при цьому $x^{(1)} = (x_t, \dots, x_1), x^{(2)} = (x_{2t}, \dots, x_{t+1}), \dots, x^{(p)} = (x_n, \dots, x_{(p-1)t+1})$. Далі позначимо $S : V_n \to V_n$ – бієктивне відображення, яке має таку структуру:

$$\forall x \in V_n : S(x) = \big(s^{(p)}\big(x^{(p)}\big), \dots, s^{(1)}\big(x^{(1)}\big)\big), \quad (1)$$

де

$$s^{(i)} : V_t \to V_t, i = \overline{1,p} \quad (2)$$

– бієктивні відображення.

Блоком підстановки будемо називати відображення, визначене за формулою (1), а відображення, визначені за формулою (2), будемо називати *вузлами заміни*, або *s-блоками*, з яких складається блок підстановки S.

З кожним s-блоком пов'яжемо наступні величини, залежні від цього s-блоку.

Лінійним потенціалом апроксимації (α, β) для довільних $\alpha, \beta \in V_t$ та s-блоку будемо називати величину

$$\lambda^{(s)}(\alpha, \beta) = \left(2^{-t} \sum_{u \in V_t} (-1)^{\beta s(u) \oplus \alpha u}\right)^2,$$

де під множенням елементів з V_t розуміється скалярне множення відповідних векторів.

[a] fenolsun@gmail.com

Максимальним потенціалом апроксимації s-блоку будемо називати величину

$$\Lambda^{(s)} = \max_{\alpha,\beta \in V_t \setminus \{0\}} \{\lambda^{(s)}(\alpha,\beta)\}$$

Коефіцієнтом Фур'є s-блоку s будемо називати величину, що для довільних $\alpha, \beta \in V_t$ та s-блоку s визначається як

$$S^W(\alpha,\beta) = \sum_{u \in V_t} (-1)^{\beta s(u) \oplus \alpha u}$$

Імовірністю диференціалу s-блоку для довільних $\alpha, \beta \in V_t$ та s-блоку s назвемо величину

$$d^{(s)}_{\oplus\oplus}(\alpha,\beta) = 2^{-t} \sum_{u \in V_t} \delta\left(s(u \oplus \alpha) \oplus s(u), \beta\right),$$

де символом δ позначено δ-функцію Кронекера.

Максимальною імовірністю диференціалу для s-блоку s будемо називати величину

$$\Delta^{(s)}_{\oplus\oplus} = \max_{\alpha,\beta \in V_t \setminus \{0\}} \{d^{(s)}_{\oplus\oplus}(\alpha,\beta)\}$$

Імовірністю цілочисельного диференціалу s-блоку для довільних $\alpha, \beta \in V_t$ та s-блоку s будемо називати величину

$$d_{\boxplus\boxplus}(s)(\alpha,\beta) = 2^{-t} \sum_{u \in V_t} \delta\left(s(u \boxplus \alpha) \boxminus s(u), \beta\right),$$

де символом $\boxplus$ позначено додавання за модулем 2^t, а символом $\boxminus$ віднімання за модулем 2^t.

Максимальною імовірністю цілочисельного диференціалу для s-блоку назвемо наступну величину:

$$\Delta^{(s)}_{\boxplus\boxplus} = \max_{\alpha,\beta \in V_t \setminus \{0\}} \{d^{(s)}_{\boxplus\boxplus}(\alpha,\beta)\}$$

Нехай $s : V_t \to V_t$ – деякий s-блок. Тоді для будь-якого аргументу $x \in V_t$ значення функції $s(x)$ може бути представлено як

$$s(x) = \big(s_t(x), \ldots, s_1(x)\big), \tag{3}$$

де $s_i : V_t \in \{0,1\}, i = \overline{1,t}$

Координатними функціями довільного s-блоку $S : V_t \to V_t$ будемо називати відображення $s_i : V_t \to \{0,1\}, i = \overline{1,t}$, визначені згідно (3).

Зокрема, координатні функції s-блоку $s^{(i)}, i = \overline{1,p}$ будемо позначати як $s^{(i)}_t, \ldots, s^{(i)}_1$. Ці координатні функції є булевими функціями, отже, кожну з них можна подати у вигляді поліному Жегалкіна.

Для довільної булевої функції $f : V_t \to \{0,1\}$ позначимо через $\deg f$ максимальний степінь її поліному Жегалкіна. Відповідно, для s-блоку $s : V_t \in V_t$ позначимо

$$\deg s = max\{\deg f_1, \ldots, \deg f_t\}$$

Вагою Хеммінга вектора $x^{(i)} \in V_t$ називається кількість одиниць у цьому векторі, яка позначається $wt\big(x^{(i)}\big)$.

Нехай $\alpha \in V_t$ – таке, що $wt(\alpha) = 1$. Тоді, якщо для будь якого s-блоку, для всіх $\beta \in V_t$, таких, що $wt(\beta) = 1$, та для всіх $k \in V_t$:

$$s(k \oplus \alpha) \oplus s(k) \neq \beta,$$

то можемо сказати, що для s-блоку виконується *властивість* Υ.

Це означає, що ймовірність переходу однобітової різниці на вході в однобітову різницю на виході дорівнює 0.

Зокрема, ця властивість присутня БСШ «Present».

Лінійним перетворенням s-блоку будемо називати перетворення π таке, що

$$\pi = A \cdot s, \tag{4}$$

де A – матриця, що належить множині всіх невироджених квадратних матриць розмірності $t \times t$ над полем F_2.

2. Постановка задачі

Для порівняння було обрано чотири шифри, зазначені у вступі. Першочерговою задачею було визначити «класичні» властивості s-блоків обраних шифрів, а саме:

1) максимальний лінійний потенціал апроксимації $\Lambda^{(s)}$;
2) максимальну ймовірність диференціалу $\Delta^{(s)}_{\oplus\oplus}$;
3) максимальну ймовірність цілочисельного диференціалу; $\Delta^{(s)}_{\boxplus\boxplus}$;
4) степінь полінома Жегалкіна $deg\ s$.

В останні роки активно розвивається модифікація класичного різницевого аналізу – цілочисельний різницевий аналіз, тому підрахунок максимальної ймовірності цілочисельної різниці $\Delta^{(s)}_{\boxplus\boxplus}$ також грає значну роль у визначенні властивостей s-блоків блокових шифрів, через що аналіз цього параметру було додано до задач.

Також не меншу зацікавленість викликає *властивість* Υ, яку потрібно перевірити для s-блоків шифрів «Калина», «BelT» та «Кузнечик».

Однією з задач було перевірити наступну властивість.

Нехай $s^{(0)}_1, \ldots, s^{(0)}_t$ – координатні функції блоку $s^{(0)}$, вектор $a = (a_t, \ldots, a_1) \in V_t \setminus \{0\}$, булева функція $\sum_{i=1}^{t} a_i s^{(0)}_i$ є лінійною комбінацією координатних функцій s-блоку $s^{(0)}$. Тоді для будь-якого вектора $a \in V_t \setminus \{0\}$ та s-блоку $s^{(0)}$ виконується

$$\deg\left(\sum_{i=1}^{t} a_i s^{(0)}_i\right) = \deg\ s^{(0)} \tag{5}$$

Рівність (5) експериментально перевірено безпосереднім перебором за всіма можливими $a = (a_t, \ldots, a_1) \in V_t \setminus \{0\}$.

Також експериментально перевірено, чи зберігаються при лінійному перетворенні властивості шифру «Present», а саме *властивість* Υ та $S^W(\alpha,\beta) = \pm 4$.

3. Результати дослідження

Перебором за всіма можливими $\alpha, \beta \in V_8$ було експериментально перевірено *властивість* Υ для s-блоків шифрів «Калина», «BelT», «Кузнечик», та для довільних $\alpha, \beta \in V_4$ для шифру «Present». Рівність (5) було також експериментально перевірено згідно поставленої задачі.

Виявлено, що *властивість* Υ виконується лише для s-блоку шифру «Present», для всіх інших s-блоків БШ, що розглядались, вона не зберігається.

Табл. 1. Порівняльна таблиця

Шифр/Властивість	$\Lambda^{(s)}$	$\Delta^{(s)}_{\oplus\oplus}$
«Калина»	$2,25 \cdot 2^{-6}$	2^{-5}
«BelT»	$2,64 \cdot 2^{-6}$	2^{-5}
«Кузнечик»	$3,0625 \cdot 2^{-6}$	2^{-5}
«Present»	2^{-2}	2^{-2}

Табл. 2. Порівняльна таблиця, продовження

Шифр/Властивість	$\Delta^{(s)}_{\boxplus\boxplus}$	$\deg s$
«Калина»	$6 \cdot 2^{-8} \ldots 8 \cdot 2^{-8}$	7
«BelT»	$7 \cdot 2^{-8}$	7
«Кузнечик»	$7 \cdot 2^{-8}$	7
«Present»	$5 \cdot 2^{-4}$	3

Рівність (5), зокрема, виконується для всіх таблиць підстановки вищезгаданих блокових симетричних шифрів.

Згідно поставленої задачі, було побудовано порівняльні таблиці 1 та 2, де значення $\Lambda^{(s)}$, $\Delta^{(s)}_{\oplus\oplus}$, $\Delta^{(s)}_{\boxplus\boxplus}$ – обраховані ймовірності. З результату можна побачити, що ці ймовірності виявилися достатньо малими для кожного s-блоку, що свідчить про стійкість до атак, заснованих на виявленнях вразливостей s-блоків через підрахунок вищезгаданих параметрів.

Було виявлено, що при лінійному перетворенні (4) s-блоку шифру «Present» *властивість* Υ та рівність $S^W(\alpha, \beta) = \pm 4$ зберігаються лише для 72 невироджених матриць A розмірності 4×4.

Висновки

Завдяки отриманим результатам можна сказати про те, що:

1) майже всі блокові шифри в якості нелінійного перетворення використовують таблиці підстановки, тому властивості s-блоків потрібно ретельно досліджувати задля забезпечення захисту інформації, що зашифровується симетричним блоковим шифром;
2) всі s-блоки стандартів, які було проаналізовано, згідно отриманим властивостям мають відносно високу стійкість до лінійного криптоаналізу, так як *максимальний потенціал апроксимації* має досить мале значення;
3) проаналізовані s-блоки шифрів зберігають степінь поліному Жегалкіна при перетворенні (5), що також показує стійкість до алгебраїчних атак;
4) визначено максимальну ймовірність цілочисельного диференціалу для кожного з обраних блокових шифрів; цей параметр грає не менш важливу роль у визначенні стійкості блокових шифрів до цілочисельного диференціального аналізу, зокрема, відома геш-функція $MD5$[6] була зламана саме завдяки вищезгаданій модифікації класичного різницевого криптоаналізу[7]. Тому, хоча й інформації щодо злому блокових симетричних шифрів за допомогою цілочисельного різницевого аналізу не було, визначення даного параметру має місце;
5) лише s-блок шифру «Present» має властивість Υ, таблиці підстановки інших стандартів, що розглядались, не зберігають цю властивість. Υ показує стійкість шифру «Present» до диференціального криптоаналізу;
6) дослідження показали, що особливі властивості, що належать s-блоку блокового шифру «Present», зберігаються при лінійному перетворенні, визначеному згідно (4), лише для деяких невироджених матриць A.

Перелік використаних джерел

1. Агиевич С. В. Алгоритм блочного шифрования BelT. — 2002. — С. 7 с. — URL: http://elib.bsu.by/bitstream/123456789/24140/1/BelT.pdf.
2. Олійников Р. В. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України. — 2015. — С. 16 с. — URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/8789/10813.
3. Сериков И. А. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры. — 2016. — URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
4. PRESENT: An Ultra-Lightweight Block Cipher / Bogdanov A., Knudsen L. R., Leander G. et al. — 2007. — P. 18. — URL: https://www.iacr.org/archive/ches2007/47270450/47270450.pdf.
5. Шеннон К. Работы по теории информации и кибернетике. — Москва : Издательство иностранной литературы, 1963. — С. 333–369. — URL: http://www.novsu.ru/file/1086154.
6. Rivest R. The MD5 Message-Digest Algorithm // RFC 1321. — 1992. — URL: https://tools.ietf.org/html/rfc1321.
7. Berson T. A. Differential cryptanalysis $mod 2^{32}$ with applications to MD5 // Advanced in Cryptology. — 1999. — P. 95–103.