

полем для построения линейных совершенных протоколов разделения одного секрета [12] и, как показано в статье, имеет меньшую временную сложность по сравнению с тривиальным алгоритмом.

Литература: 1. Введение в криптографию / Под общ. ред. В. В. Яценко. – М.: МЦНМО: “ЧеРо”, 1999. – 272 с. 2. Seberry J., Charnes C., Pieprzyk J., Safavi-Naini R. 41 Crypto topics and applications II. Handbook on Algorithms and Theory of Computation, 1998. – P. 1 – 22. 3. McLean J. Reasoning about security models // Proceeding IEEE Symposium on privacy and security. – IEEE Computer Society Press. – 1987. – P. 123-131. 4. Blakley G. R. Safeguarding cryptographic keys // Proc. AFIPS 1979 National Computer Conference. – N-Y.:1979. – V. 48. – P. 313 – 317. 5. Shamir A. How to share a secret // Comm. ACM. – 1979. – V. 22. – № 1. – P. 612 – 613. 6. Bertilsson M. Linear codes and secret sharing. – PhD Thesis. – Linköping University. – 1993. 7. Brickell E. F. Some ideal secret sharing schemes // J. Combin. Math. and Combin. Comput. – 1989. – № 9. – P. 105 – 113. 8. Blakley G. R., Kabatianski G. A. Linear algebra approach to secret sharing schemes // Preproc. of Workshop on Information Protection.: Moscow, 1993. 9. Massey J. L. Minimal codewords and secret sharing // Proc. 6th Joint Swedish-Russian Int. Workshop on Information Protection. – 1993. – P. 276 – 279. 10. Ashikhmin A., Barg A. Minimal vectors in linear codes // IEEE Trans. on Inform. Theory. – 1998. – V. 5. – P. 2010 – 2018. 11. Ashikhmin A., Barg A. Minimal vectors in linear codes and sharing of secrets // Univ. Bielefeld, SFB 343 Diskrete Strukturen in der Mathematik. – 1994. – Preprint 94 – 113, available from ftp.uni-bielefeld.de. 12. van Dijk M. A Linear construction of perfect secret sharing schemes // Advances in Cryptology – EUROCRYPT’94. – Lecture Notes in Comput. Science. – V. 950. – P. 23 – 34. 13. Simmons G. J. How to (really) share a secret // Advances in Cryptology – CRYPTO’88, Lecture Notes in Computer Science. – 1989. – Vol. 403. – P. 390 – 448. 14. Blundo C., de Santis A., di Crescenzo D., Gaggia A. G., Vaccaro U. Multi-secret sharing schemes // Advances in Cryptology – CRYPTO’94, Lecture Notes in Computer Science. – 1994. – Vol. 839. – P. 150 – 163. 15. Алексейчук А. Н., Волошин А. Л. Совершенная схема множественного разделения секрета над кольцом вычетов по модулю m // Реєстрація, зберігання і обробка даних. – 2005. – Т. 7. – № 4. – С. 44 – 53. 16. Алексейчук А. Н., Волошин А. Л., Скрипник Л. В. Совершенная схема множественного разделения секрета на основе линейных преобразований над конечным цепным коммутативным кольцом // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2 – 3 ноября 2005 г. – М.: МЦНМО, 2006. – С. 149 – 154. 17. Алексейчук А. Н., Волошин А. Л. Аналитическое описание конструкций протоколов множественного разделения секрета с многоадресным сообщением, реализующих заданную иерархию доступа // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 3. – С. 391 – 396. 18. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. – Пер. с англ. – М.: Мир, 1979. – 536 с. 19. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. Учебник. В 2-х т. Т. 1. – М.: Гелиос АРВ, 2003. – 336 с.

УДК 621.391:519.2

ОЦІНКИ ЙМОВІРНОСТЕЙ УЗАГАЛЬНЕНИХ ЛІНІЙНИХ АПРОКСИМАЦІЙ РАУНДОВОЇ ФУНКЦІЇ ГОСТ-ПОДІБНОГО БЛОКОВОГО ШИФРУ

Артур Шевцов

Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ"

Анотація: Отримані аналітичні верхні межі ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру, які залежать від певних числових параметрів його вузлів заміни. Отримані результати складають основу подальших досліджень в галузі аналізу та обґрунтування стійкості ГОСТ-подібних блокових шифрів відносно методу узагальненого лінійного криптоаналізу.

Summary: Analytical upper bounds of generalized linear approximations probabilities of the round function of a GOST-like block cipher are obtained. These bounds depends on some numerical parameters of S-boxes of the given block cipher. Obtained results form the basis for next research in area of analysis and security proving of GOST-like block ciphers against generalized linear cryptanalysis techniques.

Ключові слова: ГОСТ-подібний блоковий шифр, узагальнений лінійний криптоаналіз, узагальнена лінійна апроксимація раундової функції.

I Вступ

У процесі забезпечення конфіденційності інформації, яка циркулює в інформаційно-телекомунікаційних системах, найбільш широке застосування знаходять блокові шифри. Одними з потужних статистичних методів криптоаналізу блокових шифрів є лінійний [1] і диференціальний [2] криптоаналіз. Вони є найбільш відомими загальними методами криптографічного аналізу блокових шифрів. За останні роки відбулися якісні зміни у наукових основах цих методів, результатом яких стало більш глибоке розуміння їх сутності, ролі та положення в загальній теорії статистичних атак на блокові шифри. Обидва методи стрімко розвиваються; одночасно з'являються нові методи криптоаналізу, що є узагальненнями, об'єднаннями та комбінаціями лінійного, диференціального та інших методів [3 – 6]. Одним з таких методів є узагальнений лінійний криптоаналіз, запропонований у [5]. Зазначений метод є перспективним статистичним методом криптоаналізу блокових шифрів, який узагальнює класичний метод лінійного криптоаналізу.

Серед блокових шифрів, що наразі використовуються, практичний інтерес мають ГОСТ-подібні блокові шифри [7], найбільш відомим прикладом яких є ГОСТ 28147-89. На відміну від марковських (відносно операції \oplus порозрядного булевого додавання на множині повідомлень, що шифруються) блокових шифрів, для ГОСТ-подібних шифрів задача знаходження математично обґрунтованих оцінок параметрів, що характеризують їх практичну стійкість, є більш складною. Розв'язання даної задачі потребує розроблення нових способів побудови аналітичних оцінок параметрів, що характеризують стійкість зазначених шифрів, а саме, таких способів, що дозволяють отримувати нетривіальні оцінки їх стійкості, виходячи зі специфічних особливостей їх будови. В [7 – 9] отримані аналітичні оцінки стійкості ГОСТ-подібних блокових шифрів відносно диференціального та лінійного методів криптоаналізу. Але задача аналізу та обґрунтування стійкості таких шифрів відносно узагальненого лінійного методу криптоаналізу залишається на сьогодні невіршеною.

Зауважимо, що оцінку криптографічної стійкості будь-якого блокового шифру звичайно починають з дослідження властивостей його раундової функції. Оскільки більшість сучасних атак на блокові шифри є ітераційними, то наявність певних слабкостей раундової функції, як правило, призводить до зламування шифру. Метою даної статті є отримання математично обґрунтованих аналітичних оцінок ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру. Указані оцінки залежать тільки від числових параметрів вузлів заміни ГОСТ-подібних блокових шифрів і можуть бути безпосередньо використані на практиці при дослідженні криптографічних властивостей їх раундових функцій.

II Основні поняття та позначення

Для кожного натурального l позначимо V_l множину булевих векторів довжини l , S^{V_l} – симетричну групу підстановок на множині V_l .

Нагадаємо [7, 8], що r -раундовий ГОСТ-подібний шифр \mathfrak{S} є шифром Фейстеля з множиною відкритих (шифрованих) повідомлень V_n , де $n = 2m$, $m \geq 2$, множиною ключів $\Lambda = K^r$, множиною раундових ключів $K = V_m$ та функцією шифрування $F: V_n \times \Lambda \rightarrow V_n$ такою, що для будь-яких $x \in V_n$, $\lambda = (k(1), \dots, k(r)) \in \Lambda$ виконується рівність

$$F^{(\lambda)}(x) = F(x, \lambda) = (f^{(k(r))} \circ \dots \circ f^{(k(1))})(x), \quad (1)$$

де $f^{(k(r))} \circ \dots \circ f^{(k(1))}$ є композицією зазначених перетворень. Елементи $k(1), \dots, k(r)$ називаються раундовими ключами, а відображення $f^{(k(1))}, \dots, f^{(k(r))}$ – раундовими шифруючими перетвореннями шифру \mathfrak{S} в раундах шифрування з номерами $1, \dots, r$ відповідно. Перетворення $f^{(k)}$ ($k \in V_m$) в кожному з раундів має вигляд

$$f^{(k)}(x) = f^{(k)}(u, v) = (v, u \oplus \varphi(v + k)), \quad (2)$$

де $x = (u, v)$ – відкритий текст в даному раунді, $u, v \in V_m$, $\varphi \in S^{V_m}$, а символ \oplus позначає операцію додавання m -розрядних двійкових чисел за модулем 2^m . Крім того, вважається, що $m = pt$, $p, t \in \mathbb{N}$, і підстановка φ має наступний вигляд:

$$\varphi(z) = L(s^{(p-1)}(z^{(p-1)}), \dots, s^{(0)}(z^{(0)}))^T, \quad z = (z^{(p-1)}, \dots, z^{(0)}) \in V_m, \quad (3)$$

де $z^{(j)} \in V_t$, $s^{(j)} \in S^{V_t}$, $j \in \overline{0, p-1}$, L – оборотна матриця порядку m над полем $\mathbf{GF}(2)$. Підстановка φ називається раундовою функцією, а підстановки $s^{(j)}$ – вузлами заміни (s-блоками) шифру \mathfrak{Z} .

Введемо ряд додаткових визначень та позначень.

Нехай $g \in S^{V_l}$, $k \in V_l$, f та h – булеві функції від l змінних. Назвемо узагальненою лінійною апроксимацією підстановки g функцію $(x, y) \mapsto f(x) \oplus h(y)$, $x, y \in V_l$, а число

$$p_k^{(g)} = \mathbf{P}\{f(X) \oplus h(Y) = 0\} \quad (4)$$

– ймовірністю даної узагальненої лінійної апроксимації, яка відповідає вектору k . У рівності (4) X позначає випадковий та рівномірний двійковий вектор довжини l , а Y дорівнює $g(X + k)$. Для будь-яких $g \in S^{V_l}$, $f, h: V_l \rightarrow \{0, 1\}$ покладемо

$$l^{(g)}(f, h) = (2p_k^{(g)} - 1)^2 = 2^{-l} \sum_{k \in V_l} \left(2^{-l} \sum_{x \in V_l} \chi(f(x) \oplus h(g(x + k))) \right)^2, \quad (5)$$

$$\Lambda^{(g)}(f, h) = 2^{-l} \sum_{k \in V_l} \left(2^{-l} \sum_{a \in \{0, 1\}} \left| \sum_{\substack{x \in V_l \\ v(x, k) = a}} \chi(f(x) \oplus h(g(x + k))) \right| \right)^2, \quad (6)$$

де $\chi(u) = (-1)^u$, $u \in \{0, 1\}$, $v(x, k)$ – біт переносу в l -й розряд суми $x + k$ в кільці Z . Зауважимо, що параметр (5) характеризує ступінь близькості узагальненої лінійної апроксимації $(x, y) \mapsto f(x) \oplus h(y)$, $x, y \in V_l$, до підстановки g .

III Постановка задачі та основний результат

В роботі [5] запропоновано метод узагальненого лінійного криптоаналізу ітеративних блокових шифрів, що ґрунтується на використанні значень суми зрівноважених булевих функцій від входу та виходу раундової функції блокового шифру. Суть методу узагальненого лінійного криптоаналізу полягає у відновленні ключа в останньому раунді шифрування на основі аналізу статистичної залежності між значеннями цих функцій від відкритих і шифрованих текстів.

У [5] запропоновано використовувати метод узагальненого лінійного криптоаналізу як для зламування, так і для оцінки стійкості існуючих блокових шифрів, але при цьому не визначено відповідних показників стійкості. Тому залишається не зрозумілим, як оцінювати або обґрунтовувати стійкість блокових шифрів відносно цього методу. Теоретично обґрунтовані показники стійкості блокових шифрів відносно методу узагальненого лінійного криптоаналізу запропоновані в [10], де отримані також аналітичні верхні оцінки його надійності. Для отримання головного результату статті будемо використовувати параметр (5), застосовуючи його не до всього блокового шифру, як у [10], а лише до його раундової функції.

Задачу оцінювання стійкості ГОСТ-подібного блокового шифру \mathfrak{Z} відносно методу узагальненого лінійного криптоаналізу доцільно почати з дослідження властивостей його раундової функції з метою знаходження її найбільш ймовірних узагальнених лінійних апроксимацій, які дозволяють проводити узагальнену лінійну атаку на даний блоковий шифр. У разі відсутності зазначених апроксимацій проведення атаки з [5] на шифр \mathfrak{Z} стає неможливим. Отже, можливість здійснення такої атаки передбачає наявність алгоритму обчислення ймовірностей узагальнених лінійних апроксимацій раундової функції шифру \mathfrak{Z} .

Основна задача, яка розв'язується в даній статті, полягає у знаходженні аналітичних оцінок ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру \mathfrak{Z} , що описується співвідношеннями (1) – (3), в термінах числових параметрів, які явно залежать від s-блоків цього шифру.

Доведемо допоміжне твердження, яке встановлює верхню оцінку параметра (5) для раундової функції блокового шифру \mathfrak{Z} та певних булевих функцій f та h .

Лема. Нехай $t, m \in N$, $t \leq m-1$, $\psi_1 \in S^{V_t}$, $\psi_2 \in S^{V_{m-t}}$ та

$$\psi(x) = (\psi_2(x_2), \psi_1(x_1)), \quad x_1 \in V_t, \quad x_2 \in V_{m-t}. \quad (7)$$

Тоді для будь-яких булевих функцій вигляду $f(x) = f_2(x_2) \oplus f_1(x_1)$, $h(x) = h_2(x_2) \oplus h_1(x_1)$, $x_1 \in V_t$, $x_2 \in V_{m-t}$ виконується нерівність

$$l^{(\psi)}(f, h) \leq \Lambda^{(\psi_1)}(f_1, h_1) l^{(\psi_2)}(f_2, h_2) \leq l^{(\psi_2)}(f_2, h_2). \quad (8)$$

Доведення. Для довільних $x = (x_2, x_1)$, $k = (k_2, k_1)$, де $x_1, k_1 \in V_t$, $x_2, k_2 \in V_{m-t}$, позначимо $x = x_1 + 2^t x_2$ та $k = k_1 + 2^t k_2$ цілі числа, які відповідають зазначеним булевим векторам. Відмітимо, що $x_1, k_1 \in \overline{0, 2^t - 1}$, $x_2, k_2 \in \overline{0, 2^{m-t} - 1}$. Справедлива рівність

$$x + k = x_1 + k_1 + 2^t(x_2 + k_2 + v(x_1, k_1)), \quad x, k \in V_m, \quad (9)$$

де $v(x_1, k_1)$ – біт переносу в найстарший (t -й) розряд суми чисел x_1 та k_1 в кільці Z .

$$2^{-m} \left| \sum_{x \in V_m} \chi(f(x) \oplus h(\psi(x+k))) \right| = \begin{array}{l} \text{На підставі формул (5), (6), (7)} \\ \text{та (9) справедливі наступні} \\ \text{співвідношення:} \end{array}$$

$$\begin{aligned} &= 2^{-m} \left| \sum_{\substack{x_1 \in V_t, \\ x_2 \in V_{m-t}}} \chi[f(x_2, x_1) \oplus h(\psi_2(x_2 + k_2 + v(x_1, k_1)), \psi_1(x_1 + k_1))] \right| = \\ &= 2^{-m} \left| \sum_{x \in V_m} \chi(f_2(x_2) \oplus h_2(\psi_2(x_2 + k_2 + v(x_1, k_1)))) \chi(f_1(x_1) \oplus h_1(\psi_1(x_1 + k_1))) \right| = \\ &= \left| \sum_{a \in \{0,1\}} \left(2^{-t} \sum_{\substack{x_1 \in V_t: \\ v(x_1, k_1)=a}} \chi(f_1(x_1) \oplus h_1(\psi_1(x_1 + k_1))) \right) \left(2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(f_2(x_2) \oplus h_2(\psi_2(x_2 + k_2 + a))) \right) \right| = \\ &= \left| \sum_{a \in \{0,1\}} u_{k_1}(a) v_{k_2}(a) \right|, \end{aligned}$$

$$\text{де } u_{k_1}(a) = 2^{-t} \sum_{\substack{x_1 \in V_t: \\ v(x_1, k_1)=a}} \chi(f_1(x_1) \oplus h_1(\psi_1(x_1 + k_1))), \quad v_{k_2}(a) = 2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(f_2(x_2) \oplus h_2(\psi_2(x_2 + k_2 + a))).$$

Далі, використовуючи аргументи, аналогічні тим, що приводяться в [8], отримаємо

$$\left| \sum_{a \in \{0,1\}} u_{k_1}(a) v_{k_2}(a) \right|^2 \leq u_{k_1}(|u_{k_1}(0)| \cdot |v_{k_2}(0)|^2 + |u_{k_1}(1)| \cdot |v_{k_2}(1)|^2),$$

де $u_{k_1} = |u_{k_1}(0)| + |u_{k_1}(1)|$. Отже,

$$\begin{aligned} l^{(\psi)}(A) &= 2^{-m} \sum_{k \in V_m} \left| \sum_{a \in \{0,1\}} u_{k_1}(a) v_{k_2}(a) \right|^2 \leq 2^{-m} \sum_{\substack{k_1 \in V_t, \\ k_2 \in V_{m-t}}} u_{k_1} \sum_{a \in \{0,1\}} |u_{k_1}(a)| |v_{k_2}(a)|^2 = \\ &= 2^{-t} \sum_{k_1 \in V_t} u_{k_1} \sum_{a \in \{0,1\}} |u_{k_1}(a)| (2^{-(m-t)} \sum_{k_2 \in V_{m-t}} |v_{k_2}(a)|^2). \end{aligned} \quad (10)$$

Згідно з визначенням параметра $v_{k_2}(a)$, $k_2 \in V_{m-t}$, $a \in \{0,1\}$, справедлива рівність

$$2^{-(m-t)} \sum_{k_2 \in V_{m-t}} |v_{k_2}(a)|^2 = 2^{-(m-t)} \sum_{k_2 \in V_{m-t}} (2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(f_2(x_2) \oplus h_2(\psi_2(x_2 + k_2 + a))))).$$

В правій частині отриманої рівності зробимо заміну змінної, вважаючи $k_2' = k_2 + a$. В результаті отримаємо, що

$$2^{-(m-t)} \sum_{k_2 \in V_{m-t}} \left(2^{-(m-t)} \sum_{x_2 \in V_{m-t}} \chi(f_2(x_2) \oplus h_2(\psi_2(x_2 + k_2'))) \right)^2 = l^{(\psi_2)}(f_2, h_2).$$

Отже, на підставі формули (10), використовуючи нерівність $\Lambda^{(\psi_1)}(f_1, h_1) \leq 1$, отримаємо

$$l^{(\psi)}(f, h) \leq 2^{-t} \sum_{k_1 \in V_t} (|u_{k_1}(0)| + |u_{k_1}(1)|)^2 l^{(\psi_2)}(f_2, h_2) = \Lambda^{(\psi_1)}(f_1, h_1) l^{(\psi_2)}(f_2, h_2) \leq l^{(\psi_2)}(f_2, h_2),$$

що й треба було довести.

Доведемо тепер теорему, яка встановлює головний результат статті.

Теорема. Нехай \mathfrak{S} – ГОСТ-подібний блоковий шифр із раундовою функцією Φ вигляду (3), f_j, h_j – булеві функції від t змінних, $j \in \overline{0, p-1}$, кожна з яких є зрівноважена або тотожно дорівнює нулю $f(x) = f_{p-1}(x_{p-1}) \oplus \dots \oplus f_0(x_0)$, $h(y) = h_{p-1}(y_{p-1}) \oplus \dots \oplus h_0(y_0)$, де $x = (x_{p-1}, \dots, x_0) \in V_m$, $y = (y_{p-1}, \dots, y_0) \in V_m$, тоді виконується нерівність

$$l^{(L^{-1}\Phi)}(f, h) \leq \max \{l^{(s_j)}(f_j, h_j) : j \in \overline{0, p-1}\}. \quad (11)$$

Доведення. Покладемо $\nu = \max \{i \in \overline{0, p-1} : f_i \neq 0\}$, $\mu = \max \{j \in \overline{0, p-1} : h_j \neq 0\}$.

Тоді у випадку, коли $\nu \neq \mu$, на підставі формули (5) отримаємо, що

$$l^{(L^{-1}\Phi)}(f, h) = 0. \quad (12)$$

У випадку, коли $\nu = \mu$, справедлива рівність

$$l^{(L^{-1}\Phi)}(f, h) = l^{(L^{-1}\Phi)}(\tilde{f}, \tilde{h}), \quad (13)$$

де $\tilde{f}(x) = f_\nu(x_\nu) \oplus \dots \oplus f_0(x_0)$, $\tilde{h}(y) = h_\mu(y_\mu) \oplus \dots \oplus h_0(y_0)$, $x_i, y_j \in V_t$, $i \in \overline{0, \nu}$, $j \in \overline{0, \mu}$, з якої, внаслідок формули (8), випливає наступна нерівність:

$$l^{(L^{-1}\Phi)}(\tilde{f}, \tilde{h}) \leq \max \{l^{(s_j)}(f_j, h_j) : j \in \overline{0, p-1}\}. \quad (14)$$

Таким чином, на підставі формул (12), (13) та (14) виконується нерівність (11), що й треба було довести.

Зауважимо, що в окремому випадку, коли f та h є лінійними булевими функціями, параметр (5) співпадає з класичним показником стійкості блокових шифрів відносно методу лінійного криптоаналізу. Отже, доведена вище теорема узагальнює один з результатів статті [8], який встановлює аналітичні верхні межі ймовірностей лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру.

Як приклад застосування доведеної теореми, розглянемо раундову функцію шифру ГОСТ 28147-89. В табл. 1 представлені чисельні значення параметра

$$l^{(s)} = 2^{-l} \sum_{k \in V_l} \left(2^{-l} \sum_{x \in V_l} \chi(f(x) \oplus h(s(x+k))) \right)^2, \quad (15)$$

для одного з наборів вузлів заміни шифру ГОСТ 28147-89, що визначені в переліку довгострокових ключових елементів, які рекомендуються до застосування у засобах КЗІ Інструкцією "Про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що реалізують алгоритм, визначений ГОСТ 28147-89" [11], де $l = 4$, $\chi(u) = (-1)^u$, $u \in \{0, 1\}$, $s \in S^{V_4}$, $f = h$ – зрівноважені квадратичні булеві функції вигляду

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3 \oplus x_4.$$

Таблиця 1 – Значення параметру $l^{(s)}$ для набору довгострокових ключових елементів

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$l^{(s)}$
s_0	F	C	9	6	E	2	1	B	0	D	4	A	7	8	3	5	0,085938
s_1	E	C	5	0	7	4	A	3	2	6	1	D	9	B	F	8	0,046875
s_2	5	6	D	9	B	E	A	3	F	2	8	1	4	0	7	C	0,031250
s_3	1	F	7	4	2	E	C	3	6	B	9	8	0	5	A	D	0,054688
s_4	F	9	E	6	D	1	5	8	4	2	3	C	A	B	0	7	0,054688
s_5	B	0	D	7	C	E	1	4	2	3	6	8	A	5	F	9	0,062500
s_6	7	E	F	8	D	0	B	3	A	1	4	2	9	C	6	5	0,039062
s_7	1	5	E	B	2	C	3	8	A	0	9	7	F	6	4	D	0,093750

Проаналізувавши отримані результати для підстановок, що наведені в табл. 1, можливо зробити висновок, що значення параметра $l^{(s)}$ розподілені в діапазоні від 0,03 до 0,09. Отже, згідно з формулою (11), ймовірності узагальнених лінійних апроксимацій раундової функції шифру ГОСТ визначаються максимальними значеннями параметра $l^{(s)}$, які дають можливість проводити узагальнену лінійну атаку на шифр ГОСТ таким чином, як це описано в [5].

IV Висновки

Отримані аналітичні верхні межі ймовірностей узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного блокового шифру, які залежать від певних числових параметрів його вузлів заміни. Отримане співвідношення (11) дозволяє безпосередньо оцінювати ймовірності узагальнених лінійних апроксимацій раундової функції ГОСТ-подібного шифру \mathfrak{Z} шляхом обчислення значень параметра (5) для окремих вузлів заміни. Як приклад застосування отриманих результатів, проведені обчислення значення даного числового параметра вузлів заміни шифру ГОСТ 28147-89, що представлені в [11]. Отримані оцінки є основою для подальших досліджень з аналізу та обґрунтування стійкості ГОСТ-подібних блокових шифрів відносно методу узагальненого лінійного криптоаналізу.

Автор статті висловлює щирі подяки професору кафедри Інституту спеціального зв'язку та захисту інформації НТУУ "КПІ" А. М. Олексійчуку за корисні зауваження.

Література: 1. Matsui M. Linear cryptanalysis methods for DES cipher // *Advances in Cryptology – EUROCRYPT'93, Proceedings.* – Springer Verlag, 1994. – P. 386 – 397. 2. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // *Journal of Cryptology.* – 1991. – V. 4. – № 1. – P. 3 – 72. 3. Biryukov A. Block ciphers and stream ciphers: the state of the art // <http://eprint.iacr.org/2004/094>. 4. Biham E., Dunkelman O., Keller N. New combined attacks on block ciphers // *Fast Software Encryption. – FSE'05, Proceedings.* – Springer Verlag, 2005. – P. 126 – 144. 5. Harpes C., Kramer G. G., Massey J. L. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma // *Advances in Cryptology – EUROCRYPT'95, Proceedings.* – Springer Verlag, 1995. – P. 24 – 38. 6. Wagner D. Towards a unifying view of block cipher cryptanalysis // *Fast Software Encryption. – FSE'04, Proceedings.* – Springer Verlag, 2004. – P. 116 – 135. 7. Алексейчук А. Н. Верхние границы параметров, характеризующих стойкость немарковских блочных шифров относительно методов разностного и линейного криптоанализа // *Захист інформації.* – 2006. – № 3. – С. 20 – 28. 8. Алексейчук А. Н., Ковальчук Л. В. Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю 2^m // *Прикладная радиоэлектроника.* – 2006. – Т. 5. – № 1. – С. 74 – 82. 9. Ковальчук Л. В. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // *Материалы международной научной конференции по безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2 – 3 ноября 2005 г. М.: МЦНМО, 2006.* – С. 163 – 167. 10. Алексейчук А. Н., Шевцов А. С. Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка // *Реєстрація, зберігання і обробка даних.* – 2006. – Т. 8 – Вип. 4. – С. 53 – 63. 11. Повідомлення про оприлюднення проекту Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, що реалізують алгоритм, визначений ГОСТ 28147-89 // http://www.dststz.gov.ua/dststz/control/uk/publish/article?art_id=49003&cat_id=38710.