X Стійкість алгоритму

Стійкість алгоритму асиметричного шифрування визначається стійкістю криптографічного перетворення, визначеного в ДСТУ 4145-2002 . Нині стійкість цього перетворення дорівнює $2^{m/2}$, де m - степінь розширення основного поля. Нехай складність перебору криптографічного параметра, який шифрується за допомогою даного алгоритму, дорівнює 2^t, $t>0$. Тоді алгоритм асиметричного шифрування забезпечить адекватний захист шифрованому параметру тільки у тому випадку, якщо виконується нерівність $m \geq 2t$.

Розглянемо два практично важливих застосування цього алгоритму.

а) Шифрування сесійних ключів алгоритму ДСТУ ГОСТ 28147:2009. В цьому випадку t=256 і $m \geq 512$.

б) Шифрування довгострокових ключових елементів алгоритму ДСТУ ГОСТ 28147:2009. В цьому випадку число можливих довгострокових ключових елементів дорівнює

$$16!\cdot(16!-1)\cdots(16!-7) \approx (16!)^8 = 3{,}67\cdot 10^{106} \approx 2^{353},$$

тобто t=353 і $m \geq 706$.

Якщо нерівність $m \geq 2t$ не виконана, то стійкість криптографічних алгоритмів, що використовують криптографічні параметри, передані за допомогою алгоритму асиметричного шифрування визначатиметься не стійкістю цих криптографічних алгоритмів, а стійкістю алгоритму асиметричного шифрування. Практично у більшості випадків для шифрування сесійних ключів і довгострокових ключових елементів алгоритму ДСТУ ГОСТ 28147 : 2009 можна використовувати основне поле m=571, в особливо важливих випадках слід використовувати основне поле m=701.

XI Автентифікація повідомлення

Оскільки повідомлення, що передаються, у більшості випадків будуть блоками випадкових даних, то потрібен спосіб визначення правильності розшифрування даних. З цією метою разом із повідомленням передається 8 байтів геш-коду, обчисленого, наприклад, за допомогою алгоритму ГОСТ 34.311-95. Ймовірність випадкового збігу геш-коду спотвореного повідомлення з істинним геш-кодом дорівнює $2^{-64} \approx 10^{-18}$. Оскільки в цьому застосуванні геш-код не несе криптографічного навантаження, більше того, він шифрується разом з повідомленням, то 8 байтів геш-коду цілком достатньо для автентифікації повідомлення, що передається.

Список використаної літератури: ***1.*** *ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння»// К.: Держстандарт України, 2003. 94 с.*

Людмила Ковальчук, Наталія Кучинська, Віктор Бездітний*
*ІСЗЗІ НТУУ "КПІ", *ФТІ НТУУ "КПІ"*

УДК 621.391:519.2:519.7

ПОБУДОВА ВЕРХНІХ ОЦІНОК СЕРЕДНІХ ІМОВІРНОСТЕЙ ЦІЛОЧИСЕЛЬНИХ ДИФЕРЕНЦІАЛІВ КОМПОЗИЦІЇ МОДУЛЬНОГО КЛЮЧОВОГО СУМАТОРА, БЛОКА ПІДСТАНОВКИ ТА ЛІНІЙНОГО ОПЕРАТОРА, ЩО МАЄ БЛОКОВУ СТРУКТУРУ

Анотація: **Отримані верхні оцінки середніх імовірностей цілочисельних диференціалів для раундових функцій у випадку нетривіального блока підстановки та лінійного оператора, що має блокову структуру.**

Summary: **The upper bounds are obtained of the integer differentials average probabilities for round functions in the case of a nontrivial block permutations and a block structure linear operator.**

Ключові слова: **Різницевий криптоаналіз, диференціальний криптоаналіз, блокові шифри, раундові функції, s-блоки.**

Вступ

В представленій роботі вперше отримано верхні оцінки середніх імовірностей цілочисельних

диференціалів відображень, які є композиціями ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора, що має блокову структуру, а також визначено параметри s-блоків, від яких залежать дані оцінки, та умови, що забезпечують якомога менші значення цих оцінок. Також наведено статистичні розподіли для вказаних параметрів. Оцінки, отримані у даній роботі, є узагальненнями відповідних оцінок, отриманих у попередніх роботах [1 – 5], також вони можуть бути застосовані і в окремому випадку, коли лінійний оператор є оператором перестановки.

I Допоміжні позначення, твердження та їх доведення

Введемо для зручності наступні позначення.

Для довільного $n \in N$ позначимо через $V_n = \{0,1\}^n$ множину *n*-вимірних бітових векторів. Тут і надалі векторам з V_n будуть природнім чином поставлені у відповідність цілі числа від 0 до $2^n - 1$, тобто ми будемо ототожнювати вектори з V_n та елементи кільця Z_{2^n}.

Нехай $n = pu$, $p \geq 2$. Тоді будь-який $x \in V_n$ може бути представлений у вигляді $x = (x^{(p)},...,x^{(1)})$, де $x^{(i)} \in V_u$, $i = \overline{1,p}$.

На множині V_n введемо наступні операції та відображення. Для довільних $a,b \in V_n$ позначимо через $a+b$ ($a-b$) результат додавання (віднімання) відповідних цілих чисел за модулем 2^n, відповідно. Аналогічне позначення будемо використовувати і для операцій на множині векторів V_n (з контексту буде зрозуміло, яка саме операція мається на увазі).

Лінійний (над кільцем Z_{2^u}) оператор $A : (V_u)^p \to (V_u)^p$ задамо за допомогою матриці $A = (a_{ij})_{i,j=1}^p$, $a_{ij} \in V_u$, де для будь-якого $x = (x_p,...,x_1) \in V_n$:

$$A\,x^T = y^T = (y_p,...,y_1)^T,\ y_i = \sum_{j=1}^{p} a_{ij}x_j, \tag{1}$$

а операції множення та додавання виконуються у кільці Z_{2^u}.

Позначимо $A_i = (a_{ip},...,a_{i1})$. Тоді, в наших позначеннях, $y_i = A_i x^T$, тобто $A\,x^T = (A_p x_p,...,A_1 x_1)^T$, де під скалярним множенням розуміємо множення векторів з $(Z_{2^u})^p$.

Аналогічно позначимо $A^{-1}x^T = (A'_p x_p,...,A'_1 x_1)^T$.

Для довільного вектора $a \in (Z_{2^u})^p$ позначимо вагу Хеммінга цього вектора як $wt(a) = \#\{i : a_i \neq 0, i = \overline{1,p}\}$.

Для довільних $\beta,\gamma \in V_n$ визначимо наступні підмножини, що залежать від оператора *A*:

$$\Gamma_A(\gamma) = \{\beta \in V_n \mid \exists k \in V_n : A(k+\gamma) - A(k) = \beta\};$$
$$\Gamma_{A^{-1}}(\beta) = \{\gamma \in V_n \mid \exists k \in V_n : A(k+\gamma) - A(k) = \beta\}. \tag{2}$$

У наших позначеннях виконується наступна лема.

Лема 1: нехай $a_{ij} \in \{0,1\}$, $i,j = \overline{1,p}$. Тоді:

1) якщо оператор A такий, що $wt(A_j) \leq 2$, $j = \overline{1,p}$, то

$$\Gamma_A(\gamma) \subset \{(\beta_p,\beta_{p-1},...,\beta_1) \mid \beta_i \in \{A_i\gamma^T, A_i\gamma^T - 1, A_i\gamma^T + 1, A_i\gamma^T + 2\}, i = \overline{1,p}\};$$

2) якщо оператор *A* такий, що $wt(A'_j) \leq 2$, $j = \overline{1,p}$, то

$$\Gamma_{A^{-1}}(\beta) \subset \{(\gamma_p,\gamma_{p-1},...,\gamma_1), \mid \gamma_i \in \{A_i\beta^T, A_i\beta^T - 1, A_i\beta^T + 1, A_i\beta^T + 2\}, i = \overline{1,p}\}.$$

Доведення: нехай $\gamma, k \in V_n = (V_u)^p$.

Розглянемо різницю

$$A(k+\gamma) - A(k) = A(k_p + \gamma_p + \nu_p, ..., k_1 + \gamma_1) - A(k_p, ..., k_1),$$

де

$$\nu_i = \begin{cases} 1, & \text{якщо} \quad k_{i-1} + \gamma_{i-1} + \nu_{i-1} \geq 2^u, i \geq 2; \\ 0, & \text{інакше} \end{cases}$$

(вважаємо, що $\nu_1 = 0$). Зауважимо, що операції у цьому виразі виконуються за модулями 2^n та 2^u, залежно від того, якому векторному простору належать аргументи.

За означенням оператора A в (1) задана різниця буде дорівнювати $(\beta_p, ..., \beta_1)$, де

$$\beta_i = A_i \cdot (k_p + \gamma_p + \nu_p, ..., k_1 + \gamma_1 + \nu_1) - A_i \cdot (k_p, ..., k_1) - \mu_i,$$

та

$$\mu_i = \begin{cases} 1, & \text{якщо} \quad A_{i-1} \cdot (k_p + \gamma_p + \nu_p, ..., k_1 + \gamma_1 + \nu_1) - \mu_{i-1} < A_{i-1} \cdot (k_p, ..., k_1), \\ 0, & \text{інакше} \end{cases}$$

(вважаємо, що $\mu_1 = 0$).

Внаслідок лінійності скалярного множення над кільцем

$$\beta_i = A_i \cdot (\gamma_p, ..., \gamma_1) - A_i \cdot (\nu_p, ..., \nu_1) - \mu_i, \tag{3}$$

звідки, з урахуванням умови $wt(A_j) \leq 2,\ j = \overline{1, p}$, випливає

$$A_i \cdot (\nu_p, ..., \nu_1) \in \{0,1,2\},$$

тобто

$$A_i \cdot (\nu_p, ..., \nu_1) - \mu_i \in \{-1,0,1,2\},$$

а, отже,

$$\beta_i \in \{A_i\gamma^T, A_i\gamma^T - 1, A_i\gamma^T + 1, A_i\gamma^T + 2\}, i = \overline{1, p},$$

і перший пункт леми доведено.

Для доведення другого пункту леми зазначимо, що

$$A(k+\gamma) - A(k) = \beta \Leftrightarrow A^{-1}(\beta + A(k)) - A^{-1}(A(k)) = \gamma,$$

і далі застосуємо твердження пункту першого леми до оператора A^{-1}.

Лему доведено.

II Основні результати

Для того, аби сформулювати основні результати даної роботи, необхідні наступні позначення. Для довільної функції $F: V_n \times V_n \to V_n$ позначимо $F_k(x) := F(k, x),\ k, x \in V_n$. Будемо розглядати лише такі раундові функції, що є композиціями ключового суматора, блока підстановки та оператора перестановки:

$$F_k(x) = A(S(x+k)) \tag{4}$$

Бієктивне відображення $S: V_n \to V_n$ задамо наступним чином:

$$\forall x \in V_n: \ S(x) = (S_p(x_p), ..., S_1(x_1)), \quad x_i \in V_u, i = \overline{1, p},$$

де $S_i: V_u \to V_u, \quad i = \overline{1, p}$ – бієктивні відображення. Введене нами відображення часто називають блоком підстановки, а відображення S_i – *s*-блоками.

Згідно з [1 – 3], під середньою (за ключами) імовірністю цілочисельного диференціалу (α, β) (де $\alpha, \beta \in V_n$) функції $F: V_n \times V_n \to V_n$ будемо розуміти вираз

$$d_+^F(\alpha, \beta) = 2^{-2n} \sum_{x,k \in V_n} \delta(F_k(x+\alpha) - F_k(x), \beta). \tag{5}$$

Аналогічно до робіт [2 – 4], легко показати, що для функції $F: V_n \times V_n \to V_n$, визначеної згідно з (4), виконується рівність

$$d_+^F(\alpha,\beta) = d_+^F(0;\alpha,\beta),$$

де

$$d_+^F(0;\alpha,\beta) = 2^{-n}\sum_{k\in V_n}\delta\big(F_k(\alpha)-F_k(0),\beta\big) \tag{6}$$

– середня (за ключами) імовірність цілочисельного диференціалу (α,β) функції F у точці x=0.

Також для довільних $a,b\in V_u$ та відображення $S_i: V_u \to V_u$, $i=\overline{2,p}$ позначимо

$$\nu(a,b)=\begin{cases}1, & \text{якщо } a+b\ge 2^u;\\ 0, & \text{інакше;}\end{cases} \tag{7}$$

$$\mu^{(i)}(a,b)=\begin{cases}1, & \text{якщо } S_{i-1}(a+b)<S_{i-1}(a);\\ 0, & \text{інакше;}\end{cases} \tag{8}$$

та вважатимемо, що $\mu^{(1)}(a,b)=0$.

Для кожного $i=\overline{1,p}$ покладемо

$$\Delta_i = \max_{\alpha,\gamma\in V_n\setminus\{0\}} 2^{-u}\sum_{k\in V_u}\left(\sum_{\tau\in\{\gamma,\gamma-1,\gamma+1,\gamma+2\}}\delta\big(S_i(k+\alpha)-S_i(k),\tau\big)\right) \tag{9}$$

та

$$\Delta = \max\{\Delta_i, i=\overline{1,p}\}. \tag{10}$$

Для довільного вектора $v=(v_p,...,v_1)\in V_n$, $v_i\in V_u$, $i=\overline{1,p}$, визначимо проекційний оператор $P: V_{pu}\to V_{(p-1)u}$ за формулою $P(v)=(v_p,...,v_2)$.

У наших позначеннях справедлива наступна теорема.

Теорема 2: нехай функція F визначена за формулою (4). Тоді справедлива наступна нерівність:

$$\forall\alpha,\beta\in V_n\setminus\{0\}\quad d_+^F(\alpha,\beta)\le\Delta, \tag{11}$$

або, іншими словами,

$$\max_{\alpha,\beta\in V_n\setminus\{0\}} d_+^F(\alpha,\beta)\le\Delta. \tag{12}$$

Доведення: згідно з означенням імовірності цілочисельного диференціала та за формулою (4),

$$d_+^F(\alpha,\beta)=2^{-2n}\sum_{x,k\in V_n}\delta(F_k(x+\alpha)-F_k(x),\beta)=2^{-2n}\sum_{x,k\in V_n}\delta(A(S(x+k+\alpha))-A(S(x+k)),\beta)$$

Після заміни змінної $x+k$ на k отримаємо:

$$d_+^F(\alpha,\beta)=2^{-n}\sum_{k\in V_n}\delta(A(S(k+\alpha))-A(S(k)),\beta)=$$

$$=2^{-n}\sum_{k\in V_n}\Big\{\sum_{\gamma\in V_n}\delta(A(S(k)+\gamma)-A(S(k)),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\Big\}=$$

$$=2^{-n}\sum_{k\in V_n}\Big\{\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\delta(A(S(k)+\gamma)-A(S(k)),\beta)\times\delta(S(k+\alpha)-S(k),\gamma)\Big\}\le$$

$$\le 2^{-n}\sum_{k\in V_n}\left\{\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\delta(S(k+\alpha)-S(k),\gamma)\right\}=2^{-n}\sum_{k\in V_n}\sum_{\gamma\in\Gamma_A^{-1}(\beta)}\prod_{i=1}^{p}\delta(S_i(k_i+\alpha_i+\nu_i)-S_i(k_i)-\mu_i,\gamma_i),$$

де $\nu_i = \nu(k_{i-1}, \alpha_{i-1})$, $\mu_i = \mu^{(i)}(k_{i-1}, \alpha_{i-1} + \nu_{i-1})$.

Зауважимо, що остання нерівність отримана внаслідок того, що $\delta(A(S(k)+\gamma) - A(S(k)), \beta) \le 1$.

Для довільного $x \in V_n$, $x = (x_p, x_{p-1}, ..., x_1)$, $x_i \in V_u$, $i = \overline{1, p}$ та для введеного раніше відображення $S : V_n \to V_n$ позначимо

$$\widetilde{x} = P(x) = (x_p, x_{p-1}, ..., x_2) \in V_{n-u},\ \widetilde{S} : V_{n-u} \to V_{n-u},$$

де

$$\forall \widetilde{x} \in V_{n-u}:\ \widetilde{S}(\widetilde{x}) = P(S(x)) = (S_p(x_p), ..., S_2(x_2)),\quad x_i \in V_u,\ i = \overline{2, p},$$ і тому $x = (\widetilde{x}, x_1) \in V_n$;

для довільного $\beta \in V_n$ позначимо $T(\beta) = \{A_1'\beta^T,\ A_1'\beta^T - 1,\ A_1'\beta^T + 1,\ A_1'\beta^T + 2\}$.

Також для довільного $\alpha \in V_n$ позначимо $i = \min\{j = \overline{1, p} : \alpha_j \ne 0\}$.

Розглянемо наступні випадки.

Випадок 1. Нехай $i = 1$. Тоді $\gamma = (\widetilde{\gamma}, \gamma_1) \in \Gamma_A^{-1}(\beta)$ та $\gamma_1 \in T(\beta)$. Тоді

$$d_+^F(\alpha, \beta) \le 2^{-(n-u)} \sum_{\widetilde{k} \in V_{n-u}} 2^{-u} \sum_{k_1 \in V_u} \left[\left(\sum_{\widetilde{\gamma} \in P(\Gamma_A^{-1}(\beta))} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \nu_2) - \widetilde{S}(\widetilde{k}) - \mu_2, \widetilde{\gamma}) \right) \times \right.$$

$$\left. \times \left(\sum_{\gamma_1 \in T(\beta)} \delta(S_1(k_1 + \alpha_1) - S_1(k_1), \gamma_1) \right) \right].$$

Зазначимо, що при кожній фіксованій парі $\widetilde{k} \in V_{n-u}$ та $k_1 \in V_u$ в сумі

$$\sum_{\widetilde{\gamma} \in P(\Gamma_A^{-1}(\beta))} \delta(\widetilde{S}(\widetilde{k} + \widetilde{\alpha} + \nu_2) - \widetilde{S}(\widetilde{k}) - \mu_2, \widetilde{\gamma})$$

буде не більше одного ненульового доданку, тому ця сума не перевищує одиниці. Звідси

$$d_+^F(\alpha, \beta) \le 2^{-(n-u)} \sum_{\widetilde{k} \in V_{n-u}} 2^{-u} \sum_{k_1 \in V_u} \left(\sum_{\gamma_1 \in T(\beta)} \delta(S_1(k_1 + \alpha_1) - S_1(k_1), \gamma_1) \right) =$$

$$= 2^{-u} \sum_{k_1 \in V_u} \left(\sum_{\gamma_1 \in T(\beta)} \delta(S_1(k_1 + \alpha_1) - S_1(k_1), \gamma_1) \right).$$

Враховуючи позначення (10) та (11), отримаємо $d_+^F(\alpha, \beta) \le \Delta_1 \le \Delta$.

Випадок 2. Нехай тепер $1 < i \le p$, тобто

$$\alpha = (\alpha_p, \alpha_{p-1}, ..., \alpha_i, 0, ..., 0),\quad \alpha_j \in V_u,\quad j = \overline{1, p}.$$

Тоді, внаслідок бієктивності відображення $S : V_n \to V_n$ з умови $\delta(S(k+\alpha) - S(k), \gamma) \ne 0$ випливає умова $\gamma_1 = ... = \gamma_{i-1} = 0$, тобто $\gamma = (\gamma_p, ..., \gamma_i, 0, ..., 0)$. Виконуючи перетворення, аналогічні до наведених у випадку 1, але вже для *i*-го s-блоку замість першого, отримаємо нерівність:

$$d_+^F(\alpha, \beta) \le \Delta_i \le \Delta.$$

Отже, в загальному випадку буде справедлива нерівність

$$d_+^F(\alpha, \beta) \le \Delta.$$

Теорему доведено.

III Статистичний розподіл параметрів s-блоків

Наведемо статистичний розподіл параметрів s-блоків, від яких залежать отримані у цьому розділі верхні оцінки.

Для отримання статистичного розподілу параметра (11) було вибрано 100000 випадкових восьмибітових s-блоків (перестановок). Перестановки генерувались методом безповторного набору. У наступній таблиці наведено цей розподіл.

Таблиця 1 – Статистичний розподіл параметру Δ (вибірка з 100000 випадкових восьмибітових s-блоків)

Значення Δ_2	Значення $2^8 \cdot \Delta_2$	Кількість	Імовірність
0,046875	12	239	0,00239
0,050781	13	16459	0,16459
0,054688	14	45436	0,45436
0,058594	15	26832	0,26832
0,0625	16	8346	0,08346
0,066406	17	2078	0,02078
0,070313	18	483	0,00483
0,074219	19	102	0,00102
0,078125	20	21	0,00021
0,082031	21	4	0,00004

IV Висновки

В даній статті вперше отримано верхні оцінки середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та довільного лінійного (над деяким кільцем) оператора, який має блокову структуру. Також отримано, строго обґрунтовані, параметри, що залежать від s-блоків та характеризують дані оцінки, та побудовано статистичний розподіл даних параметрів.

Отримані результати дозволяють аналізувати різницеві властивості раундових функцій блокових алгоритмів шифрування, що мають відповідну структуру. Зауважимо, що стійкість всього блокового алгоритму до різницевого аналізу залежить від різницевих властивостей його раундових функцій.

Для подальшого дослідження є цікавими та актуальними наступні задачі.

1. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та оператора перестановки у випадку, коли у ключовому суматорі реалізована операція побітового додавання.
2. Побудова аналогічних оцінок (у випадку довільного ключового суматора) для "змішаних" диференціалів з різними операціями на вході та виході.
3. Отримання відповідних параметрів, що залежать від s-блоків та характеризують дані оцінки. Побудова статистичного розподілу вказаних параметрів та аналіз даного розподілу.
4. Побудова аналогічних оцінок для композиції ключового суматора, блоку підстановки та оператора, лінійного відносно побітового додавання.
5. Порівняльний аналіз операцій покомпонентного та модульного додавання на множині векторів над простим скінченим полем.

Список використаної літератури: ***1.*** *Ковальчук Л. Обобщённые марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-06), 25-27 октября 2006. – С. 595-599.* ***2.*** *Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. //«Кибернетика и системный анализ» – 2010, – №6, С. 89 – 96.* ***3.*** *Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. //«Кибернетика и системный анализ» – 2012, – №5, С. 71 – 81.* ***4.*** *Кучинская Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига. // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №1 (23), С. 18 – 24.* ***5.*** *Кучинская Н. В., Скрыпник Л. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов для раундовых функций определенной структуры // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації» – 2013, – №2 (24), С. 26 – 32.*