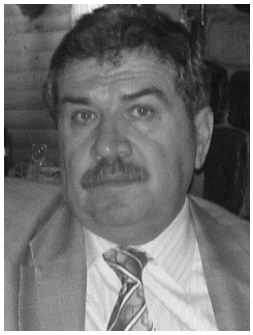
ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.26.14876

АНАЛІЗ ОПЕРАЦІЙ МОДУЛЬНОГО ТА ПОКОМПОНЕНТНОГО ДОДАВАННЯ У БЛОКОВИХ ШИФРАХ

Геннадій Гулак

Інститут проблем математичних машин і систем Національної академії наук України



ГУЛАК Геннадій Миколайович, к.т.н., доцент

Рік та місце народження: 1955, РК.
Освіта: Вища школа КДБ СРСР.
Посада: завідувач лабораторії досліджень кібербезпеки Інституту проблем математичних машин і систем Національної академії наук України.
Наукові інтереси: криптографія, кібербезпека та інформаційна безпека, гарантоздатні системи.
Публікації: 25 наукових публікацій, 5 навчальних посібників.
E-mail: h.hulak@ukr.net.
Orcid ID: 0000-0001-9131-9233.

Анотація У роботі досліджуються властивості операцій модульного та покомпонентного додавання, що використовуються у вузлах блокових шифрів, які забезпечують додавання ключової інформації (ключові суматори), та їх вплив на практичну криптографічну стійкість. Для цього отримані допоміжні результати щодо функцій розподілу імовірностей звичайних та модульних сум незалежних рівномірно розподілених випадкових величин. В основній частині доведено що послідовність бітів переносу в наступний розряд при модульному додаванні чисел $a, b \in Z_{p^n}$, утворюють однорідний ланцюг Маркова з визначеним початковим станом та відповідною матрицею переходів, а також обчислена імовірність того, що при модульному та покомпонентному додаванні в результаті утвориться $k < n$-1 переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають. З урахуванням допоміжних результатів у статті отриманні та порівняні імовірнісні характеристики операцій покомпонентного та модульного додавання (віднімання), обчислені імовірності співпадіння результатів зазначених операцій, зроблені висновки щодо коректності (некоректності) використання відповідних модифікацій блокових шифрів для побудови оцінок стійкості, наведені практично застосовні зразки блоків заміни до блокових шифрів, які відповідають визначеним умовам, визначена можливість вразливості шифру до певних типів різницевих атак за умови наявності додаткової інформації щодо того, що при оцінці стійкості даного шифру використовувалась його модифікація, отримана шляхом заміни операції у ключовому суматорі на деяку іншу. У статті обґрунтовані висновки, що заміна операції у ключовому суматорі або блоку підстановки шифру недопустима без попередніх досліджень, що полягають в обчисленні і порівнянні відповідних параметрів.

Ключові слова: блоковий шифр, блок заміни, ключовий суматор, операція модульного додавання, операція покомпонентного додавання, криптографічна стійкість

Вступ

У якості механізму забезпечення конфіденційності інформації, контролю її цілісності, а також реалізації процедур автентифікації, генерації ключами та управління ними в гарантоздатних інформаційних системах різного призначення широко використовуються симетричні криптосистеми. Серед означених криптосистем особливе місце займають блокові шифри (далі – БШ), які, зазвичай, спеціально проектуються для застосування у системах захисту інформації в комп'ютерних мережах, автоматизованих системах управління тощо [1] - [3].

Головною характеристикою застосовності БШ для виконання перелічених вище функцій є їх практична криптографічна стійкість, яка визначається у ході проектування та досліджень цих шифрів для всіх відомих на поточний час видів криптоаналітичних атак [2] – [4].

Практична стійкість криптографічних алгоритмів є базовою умовою безпеки засобів захисту, в яких вони вбудовані, але особливості програмної або апаратної реалізації можуть утворювати небезпечні стани у роботі цих засобів, внаслідок чого можуть бути викривлені вхідні дані або структурні елементи цих алгоритмів, що може призвести до суттєвого зниження рівня безпеки криптографічних перетворень [5] – [7]. В свою чергу, зниження рівня інформаційної безпеки або кібербезпеки засобів криптографічного захисту інформації може мати наслідком зниження рівня функціональної безпеки інформаційної системи, отже – її гарантоз-

датності. Окремо слід зазначити, що під час виробництва засобів захисту або їх експлуатації некоректна зміна параметрів та елементів криптографічної схеми також може мати негативні наслідки для гарантоздатності інформаційної системи [5], [8].

Таким чином, у ході проектування та досліджень засобів криптографічного захисту інформації вкрай необхідно враховувати припустимі межі зміни параметрів або елементів криптогріфчних алгоритмів у разі випадкових факторів (помилка проектанта, збій/ відмова засобу) або навмисних впливів (втручання інсайдерів/ зловмисників). У визначених умовах у випадку БШ об'єктами особливої уваги постають раундові операції з ключовими даними та блоки заміни [3], [4]

Слід зазначити, що проектування сучасних БШ ґрунтується на визначених у роботі К. Шеннона [9] принципах розсіювання *(diffusion)* та перемішування *(confusion)*. Такі принципи передбачають, що під час проектування шифру забезпечується вплив кожного знаку ключа або відкритого тексту на багато знаків шифрованого тексту, а також побудову криптографічного перетворення таким чином, щоб максимально ускладнити відновлення алгебраїчних та статистичних зв'язків між від відкритим текстом, ключем та шифрованим текстом. Тому найбільш поширеним методом побудови сучасних БШ для комп'ютерних систем є метод, заснований на застосуванні ітераційних схем [3], в яких криптографічне перетворення реалізується шляхом суперпозиції багато разів повторюваних простих з точки зору обчислювальної складності перетворень, кожне з яких вносить певний внесок в сумарне розсіювання і перемішування. В зв'язку з цим виникає питання про знаходження такого набору операцій на множині бітових векторів (відкритих текстів), які, з одного боку, зручно реалізуються програмним або апаратним способом, а з іншого – мають «хороші» перемішуючі та розсіювачі властивості [10]-[15].

З іншого боку, при оцінюванні стійкості БШ до різних методів криптоаналізу (зокрема, до лінійного та різницевого) дослідники іноді намагаються замість вихідного шифру використовувати його спрощену модель. При цьому, автори зменшують кількість раундів БШ, змінюють ключовий розклад, а особливо часто замінюють (явно або неявно) модульне додавання у ключовому суматорі на покомпонентне (побітове). Таке спрощення найчастіше використовується для алгоритмів ГОСТ 28147-89, "Мухомор", "Калина" [16] - [18]. Там операція додавання за модулем 2^{32} замінюється операцією побітового додавання, що суттєво спрощує криптоаналіз. Якихось обґрунтованих аргументів стосовно математичної коректності такої заміни у роботах не наводиться; лише деякі міркування відносно того, що при заміні нелінійної (відносно $\oplus$) операції на лінійну стійкість алгоритму не зростає. Оскільки такі міркування зустрічаються досить часто, то постає питання: "Чи можна при оцінці криптографічної стійкості алгоритму замінювати одну операцію на іншу, отримуючи при цьому еквівалентний у сенсі криптостійкості алгоритм?". Саме відповіді на це питання, а також на деякі суміжні з ним, присвячена дана робота.

Тому актуальність даної роботи визначається необхідністю обґрунтування можливості використання модифікацій БШ з заміною операції у ключовому суматорі або, навпаки, обґрунтуванням некоректності такої заміни.

Метою даної роботи є отримання та порівняння імовірнісних характеристик операцій покомпонентного та модульного додавання, отримання імовірностей співпадіння результатів цих операцій, формування висновків щодо коректності використання відповідних моделей БШ для оцінки стійкості вихідного алгоритму, а також виявлення можливої вразливості шифру до певних типів різницевих атак за умови наявності додаткової інформації щодо того, що при оцінці стійкості даного шифру використовувалась його модифікація, отримана шляхом заміни операції у ключовому суматорі на деяку іншу.

Схожі питання для побітових операцій розглянуті в [18], проте у цій роботі отримано узагальнення її результатів на випадок довільного простого модуля p, але лише в частковому випадку двох доданків.

1. Допоміжні позначення та результати

При доведенні основних результатів будуть використовуватись наступні позначення та твердження. Тут і надалі під $\left(V_n(p), \oplus_p\right)$ будемо розуміти множину векторів довжини n з операцією покомпонентного додавання за модулем простого числа p, а під $\left(Z_{p^n}, +\right)$ – адитивну групу кільця лишків з операцією додавання за модулем p^n. Кожному цілому числу $z \in Z_{p^n}$ поставимо у відповідність вектор довжини n, що є p-арним поданням цього числа. Таким чином, ми ототожнюємо множини Z_{p^n} та $V_n(p)$. Ціле число та відповідний йому p-арний вектор ми будемо позначати однаково; з контексту буде зрозуміло, яке саме подання мається на увазі.

Для будь-якого $t \geq 0$ введемо наступні позначення:

$$s_t = \left(\frac{1}{2} + \frac{1}{2p^t}\right); \quad q_t = 1 - s_t.$$

Лема 1: нехай випадкові величини x та y рівноімовірно розподілені на множині $\{0, \ldots, a-1\}$, $a \in N$. Тоді

$$P(x + y < a) = P(x + y \geq a - 1) = \frac{1}{2} + \frac{1}{2a};$$

$$P(x + y < a - 1) = P(x + y \geq a) = \frac{1}{2} - \frac{1}{2a}.$$

Доведення. За формулою повної імовірності,

$$P(x+y<a)=\sum_{i=0}^{a-1}P(x+y<a/y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i)=\frac{1}{a}\sum_{j=1}^{a}P(x<j)=\frac{1}{a}\sum_{j=1}^{a}\frac{j}{a}=\frac{1}{a^2}\cdot\frac{(a+1)\cdot a}{2}=\frac{a+1}{2a}=\frac{1}{2}+\frac{1}{2a}.$$

Аналогічно доведемо друге твердження леми:

$$P(x+y<a-1)=$$

$$\sum_{i=0}^{a-1}P(x+y<a-1/y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i-1)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i-1)=\frac{1}{a}\sum_{j=0}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}\frac{j}{a}=$$

$$=\frac{1}{a^2}\cdot\frac{(a-1)\cdot a}{2}=\frac{a-1}{2a}=\frac{1}{2}-\frac{1}{2a}.$$

Оскільки

$$P(x+y<a)=1-P(x+y\ge a)=\frac{1}{2}+\frac{1}{2a}$$

та

$$P(x+y<a-1)=1-P(x+y\ge a-1)=\frac{1}{2}-\frac{1}{2a},$$

то

$$P(x+y\ge a)=P(x+y<a-1)=\frac{1}{2}-\frac{1}{2a}$$

і

$$P(x+y\ge a-1)=P(x+y<a)=\frac{1}{2}+\frac{1}{2a}.$$

Лему доведено.

Лема 2: нехай випадкові величини *x* та *y* рівноімовірно розподілені на групі $\left(Z_{p^n},+\right)$. Тоді

$$P(x\le y)=\frac{1}{2}+\frac{1}{2p^n}=s_n;\ P(x>y)=\frac{1}{2}-\frac{1}{2p^n}=q_n.$$

Доведення: позначимо $s=P(x>y)$. Зазначимо, що $P(x=y)=\frac{p^n}{p^{2n}}=\frac{1}{p^n}$. Знайдемо *s*. Використовуємо те, що $P(x\le y)=1-P(x>y)$; тоді

$$P(x<y)+P(x=y)=1-P(x>y).$$

Оскільки $P(x>y)=P(x<y)=s$, отримаємо рівність $s+\frac{1}{p^n}=1-s$, звідки $s=\frac{1}{2}-\frac{1}{2p^n}$.

Тоді

$$P(x>y)=s=\frac{1}{2}-\frac{1}{2p^n}\ ,\text{ а}$$

$$P(x\le y)=1-P(x>y)=1-s=1-\left(\frac{1}{2}-\frac{1}{2p^n}\right)=\frac{1}{2}+\frac{1}{2p^n}.$$

В наших позначеннях,

$$P(x>y)=\frac{1}{2}-\frac{1}{2p^n}=q_n\ \text{ та }\ P(x\le y)=\frac{1}{2}+\frac{1}{2p^n}=s_n.$$

Лему доведено.

2. Порівняння операцій модульного та покомпонентного додавання

Введемо наступні позначення. Нехай $m,n,p\in N$; зазвичай через *p* ми будемо позначати просте число.

Нехай $a,b\in Z_{p^n}$, $a=(a_{n-1},...,a_0), b=(b_{n-1},...,b_0)$.

Позначимо $z=(z_{n-1},...,z_0)$, де $z=(a+b)\bmod p^n$, та $y=(y_{n-1},...,y_0)$, де $y_i=(a_i+b_i)\bmod p$.

Також позначимо:

$$\nu_0=0,$$

$$\nu_i=\begin{cases}0, \text{ якщо } a_{i-1}+b_{i-1}+\nu_{i-1}<p,\\ 1, \text{ інакше,}\end{cases}$$

де $i=1,...,n-1$.

Зрозуміло, що ν_i є бітом переносу в наступний розряд при модульному додаванні чисел *a* та *b*.

Також ми будемо використовувати позначення розділу I.

В наших позначеннях справедлива наступна лема.

Лема 3: нехай випадкові величини *a* та *b* рівноімовірно розподілені Z_{p^n}. Тоді:

$$P(\nu_i=0)=s_i,\ P(\nu_i=1)=q_i,\ i=\overline{1,n}.$$

Доведення: з означення ν_i випливає, що

$$P(\nu_i=0)=P(\overline{a_{i-1}a_{i-2}...a_0}+\overline{b_{i-1}b_{i-2}...b_0}<p^i).$$

Тоді, за лемою 1, $P(\nu_i=0)=s_i, i=\overline{1,n}$.

Аналогічно, $P(\nu_i=1)=1-s_i=q_i, i=\overline{1,n}$.

Лему доведено.

З використанням леми 3 можна довести наступну теорему.

Теорема 4: послідовність $\nu_i, i\ge 1$, утворює однорідний ланцюг Маркова з початковим станом $\nu_0=0$ та з матрицею переходів

$$P=(p_{ij})_{i,j=1}^{2},$$

де $p_{00}=p_{11}=s_1;\ p_{01}=p_{10}=q_1$.

Доведення: за означенням,

$$P(\nu_i=0)=P(a_{i-1}+b_{i-1}+\nu_{i-1}<p),$$

$$P(\nu_i=1)=1-P(\nu_i=0).$$

Тому $P(\nu_i=a/\nu_{i-1,...,\nu_1})=P(\nu_i=a/\nu_{i-1})$,

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

$$P_{11}=P(\nu_i=1/\nu_{i-1}=1)=P(a_{i-1}+b_{i-1}+1\ge p)=P(a_{i-1}+b_{i-1}\ge p-1)=\frac{1}{2}+\frac{1}{2p}=s_1;$$

$$P_{01}=P(\nu_i=1/\nu_{i-1}=0)=P(a_{i-1}+b_{i-1}\ge p)=\frac{1}{2}-\frac{1}{2p}=q_1;$$

$$P_{10}=P(\nu_i=0/\nu_{i-1}=1)=P(a_{i-1}+b_{i-1}+1<p)=P(a_{i-1}+b_{i-1}<p-1)=\frac{1}{2}-\frac{1}{2p}=q_1;$$

$$P_{00}=P(\nu_i=0/\nu_{i-1}=0)=P(a_{i-1}+b_{i-1}<p)=\frac{1}{2}+\frac{1}{2p}=s_1.$$

Теорему доведено.

Сформулюємо наслідки з теореми 4.

Наслідок 5: позначимо $p_i = P(y_i = z_i)$. Тоді $p_i = \frac{1}{2} + \frac{1}{2p^i}$, тобто $p_i \to \frac{1}{2}, i \to \infty$.

Доведення: за лемою 1, $P(y_i = z_i) = P(\nu_i = 0) = \frac{1}{2} + \frac{1}{2p^i}$. Наслідок доведено.

Наслідок 6: у наших позначеннях

$$P(y = z) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Доведення: так як послідовність ν_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\nu_0 = 0$, маємо:

$$P(y = z) = P(\bigcap_{i=0}^{n-1}\{y_i = z_i\}) = P(y_{n-1} = z_{n-1} \Big/ y_0 = z_0, ..., y_{n-2} = z_{n-2}) \times$$
$$P(y_{n-2} = z_{n-2} \Big/ y_0 = z_0, ..., y_{n-3} = z_{n-3}) \cdot ... \cdot P(y_1 = z_1 \Big/ y_0 = z_0) =$$
$$P(\nu_{n-1} = 0 \Big/ \nu_0 = 0, ..., \nu_{n-2} = 0) \times$$
$$P(\nu_{n-2} = 0 \Big/ \nu_0 = 0, ..., \nu_{n-3} = 0) \cdot ... \cdot P(\nu_1 = 0 \Big/ \nu_0 = 0) \cdot P(\nu_0 = 0) =$$
$$P(\nu_{n-1} = 0 \Big/ \nu_{n-2} = 0) \times$$
$$P(\nu_{n-2} = 0 \Big/ \nu_{n-3} = 0) \times ... \times P(\nu_1 = 0 \Big/ \nu_0 = 0) \cdot 1 = s_1^{n-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Наслідок доведено.

Наслідок 7: у наших позначеннях справедлива рівність:

$$P(y_0 = z_0,\ y_1 = z_1, ...,\ y_{k-1} = z_{k-1},\ y_k \neq$$
$$z_k,\ y_{k+1} \neq z_{k+1},\ ...,\ y_{n-1} \neq z_{n-1}) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right),$$

де $k = 1,...,n-1$.

Доведення: за формулою множення імовірностей,

$$P(y_0 = z_0, y_1 = z_1, ..., y_{k-1} = z_{k-1}, y_k \neq$$
$$z_k, y_{k+1} \neq z_{k+1}, ..., y_{n-1} \neq z_{n-1},) =$$
$$P(\nu_0 = 0) \cdot P(\nu_1 = 0 \Big/ \nu_0 = 0) \times$$
$$\times P(\nu_2 = 0 \Big/ \nu_1 = 0) \cdot ... \cdot P(\nu_{k-1} = 0 \Big/ \nu_{k-2} = 0) \cdot$$
$$P(\nu_k = 1 \Big/ \nu_{k-1} = 0) \cdot P(\nu_{k+1} = 1 \Big/ \nu_k = 1) \cdot$$
$$P(\nu_{k+2} = 1 \Big/ \nu_{k+1} = 1) \cdot ... \times$$
$$\times P(\nu_{n-1} = 1 \Big/ \nu_{n-2} = 1) =$$
$$1 \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right) \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} =$$
$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right).$$

Наслідок 8: імовірність того, що при модульному та покомпонентному додаванні в результаті утвориться $k < n-1$ переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають, визначається наступною формулою:

$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right)^{k}.$$

Доведення здійснюється аналогічно доведенню наслідку 7.

3. Порівняння результатів операцій модульного та покомпонентного віднімання

Позначимо $w = (w_{n-1}, ..., w_0)$, де $w = (a-b) \bmod p^n$ та $u = (u_{n-1}, ..., u_0)$, де $u_i = (a_i - b_i) \bmod p$.

Також позначимо:

$$\mu_i = 0;$$
$$\mu_i = \begin{cases} 0, \text{ якщо } a_{i-1} - \mu_{i-1} \geq b_{i-1} \\ 1, \text{ інакше.} \end{cases}, i = 1..n-1.$$

Зрозуміло, що μ_i є бітом запозичення в наступному розряді при модульному відніманні чисел *a* та *b*.

Також ми будемо використовувати позначення пункту 1.

В наших позначеннях справедлива наступна лема:

Лема 9: нехай випадкові величини *a, b* рівноімовірно розподілені на Z_{p^n}. Тоді:

$$P(\mu_i = 0) = s_i,\ P(\mu_i = 1) = q_i,\ i = \overline{1,n}.$$

Доведення: з означення μ_i, випливає, що

$$P(\mu_i = 0) = P(\overline{a_{i-1}a_{i-2}...a_0} \geq \overline{b_{i-1}b_{i-2}...b_0}).$$

Тоді, за лемою 2,

$$P(\mu_i = 0) = s_i, i = \overline{1,n}.$$

Аналогічно,

$$P(\mu_i = 1) = 1 - s_i = q_i, i = \overline{1,n}.$$

З використанням леми 9 можна довести наступну теорему.

Теорема 10: послідовність μ_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\mu_0 = 0$ та з матрицею переходів

$$P = (p_{ij})_{i,j=1}^{2},$$

де $p_{00} = p_{11} = s_1;\ p_{01} = p_{10} = q_1$.

Доведення: за означенням,

$$P(\mu_i = 0) = P(a_{i-1} - \mu_{i-1} \geq b_{i-1}),$$
$$P(\mu_i = 1) = 1 - P(\mu_i = 0).$$

Тому

$$P(\mu_i = a / \mu_{i-1},...,\mu_0) = P(\mu_i = a / \mu_{i-1}),$$

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

$$P_{11} = P(\mu_i = 1 / \mu_{i-1} = 1) =$$

$$P(a_{i-1} - 1 < b_{i-1}) = P(a_{i-1} < b_{i-1} + 1) =$$

$$= \sum_{k=0}^{p-1} P\left(a_{i-1} < b_{i-1} + 1 / a_{i-1} = \kappa\right) \cdot P(a_{i-1} = \kappa) =$$

$$\sum_{k=0}^{p-1} P\left(k < b_{i-1} + 1\right) \cdot P(a_{i-1} = k) =$$

$$= \frac{1}{p} \cdot (p + p - 1 + p - 2 + ... + 1) \cdot \frac{1}{p} =$$

$$\frac{1}{p} \cdot \frac{1+p}{2} \cdot p \cdot \frac{1}{p} = \frac{1}{2p} + \frac{1}{2} = s_1;$$

$$P_{01} = P(\mu_i = 1 / \mu_{i-1} = 0) = P(a_{i-1} < b_{i-1}) = \frac{1}{2} - \frac{1}{2p} = q_1;$$

$$P_{10} = P(\mu_i = 0 / \mu_{i-1} = 1) =$$

$$P(a_{i-1} - 1 \geq b_{i-1}) =$$

$$1 - P(a_{i-1} - 1 < b_{i-1}) =$$

$$1 - (\frac{1}{2} + \frac{1}{2p}) = \frac{1}{2} - \frac{1}{2p} = q_1;$$

$$P_{00} = P(\mu_i = 0 / \mu_{i-1} = 0) = P(a_{i-1} \geq b_{i-1}) = \frac{1}{2} + \frac{1}{2p} = s_1.$$

Теорему доведено.

Сформуємо наслідки з теореми 10.

Наслідок 11: позначимо $p_i = P(w_i = u_i)$.

Тоді $p_i = \frac{1}{2} + \frac{1}{2p^i}$, тобто $p_i \to \frac{1}{2}, i \to \infty.$

Доведення:

За лемою 2, $P(w_i = u_i) = P(\mu_i = 0) = \frac{1}{2} + \frac{1}{2p^i}$.

Наслідок доведено.

Наслідок 12: у наших позначеннях

$$P(w = u) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Доведення: так як послідовність μ_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\mu_0 = 0$, маємо:

$$P(w = u) = P(\bigcap_{i=0}^{n-1} \{w_i = u_i\}) =$$

$$= P(w_{n-1} = u_{n-1} / w_0 = u_0, ..., w_{n-2} = u_{n-2}) \cdot$$

$$P(w_{n-2} = u_{n-2} / w_0 = u_0, ..., w_{n-3} = u_{n-3}) \cdot ... \cdot$$

$$P(w_1 = u_1 / w_0 = u_0) =$$

$$= P(\mu_{n-1} = 0 / \mu_0 = 0, ..., \mu_{n-2} = 0) \cdot$$

$$P(\mu_{n-2} = 0 / \mu_0 = 0, ..., \mu_{n-3} = 0) \cdot ... \cdot$$

$$P(\mu_1 = 0 / \mu_0 = 0) \cdot P(\mu_0 = 0) =$$

$$= P(\mu_{n-1} = 0 / \mu_{n-2} = 0) \cdot P(\mu_{n-2} = 0 / \mu_{n-3} = 0) \cdot ... \cdot$$

$$P(\mu_1 = 0 / \mu_0 = 0) \cdot 1 = s_1^{n-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Наслідок доведено.

Наслідок 13: у наших позначеннях виконується рівність

$$P(w_0 = u_0, w_1 = u_1, ..., w_{k-1} = u_{k-1}, w_k \neq u_k, w_{k+1} \neq u_{k+1}, ..., w_{n-1} \neq u_{n-1},) =$$

$$= \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right),$$

Доведення наслідку здійснюється аналогічно доведенню наслідку 6.

Наслідок 14: імовірність того, що при модульному та покомпонентному відніманні в результаті утвориться $k < n$-1 переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають, визначається наступною формулою:

$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right)^{k}.$$

Доведення здійснюється аналогічно доведенню наслідку 13.

4 Загрози зменшення криптографічної стійкості шифру у разі некоректної заміни його окремих компонент

Як видно з попередніх розділів, результати операцій побітового та модульного додавання суттєво відрізняються. Це призводить до висновку, що різницеві характеристики перетворень, які є складовими шифру, теж можуть суттєво відрізнятись при різних вхідних/вихідних операціях. Зокрема цей факт ще раз підтверджує, що стійкість шифру до класичного (побітового) різницевого криптоаналізу не гарантує його стійкість до цілочисельного, і навпаки. Але, крім цього, цю особливість взаємної поведінки операцій можна також використати для внесення певних змін в структуру шифру, що призведуть до навмисного погіршення його різницевих характеристик. Важливо, що при цьому користувач шифру буде вважати, що зміни внесено для покращення різницевих властивостей шифру. Далі розглянемо декілька ситуацій з внесенням таких змін.

Введемо 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 ставитись у відповідність цілі числа від 0 до $2^n - 1$, $n \in N$.

Якщо $n = pu, \quad p \geq 2,$ то будь-який $x \in V_n$ може бути поданий у вигляді $x = (x^{(p)}, ..., x^{(1)})$, $x^{(i)} \in V_u, \quad i = \overline{1, p}$.

На множині V_n введемо наступні операції та відображення. Для довільних $a,b \in V_n$ через $a \oplus b$ будемо позначати результат побітового додавання векторів *a* та *b*, а через $a+b$ та $a-b$ відповідно результати додавання та віднімання цілих чисел за модулем 2^n.

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. Це відображення часто називають блоком підстановки, а відображення $S^{(i)}$ – *s*-блоками.

Нехай $L: V_n \to V_n$ – лінійний оператор.

Для довільної функції $F: V_n \times V_n \to V_n$ позначимо $F_k(x) := F(k, x), \ k, x \in V_n$. Ми будемо розглядати шифри, у яких раундові функції мають вигляд

$$F_k(x) = L\big(S(x \oplus k)\big) \text{ або } F_k(x) = L\big(S(x + k)\big). \quad (1)$$

Для довільного s-блока покладемо

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

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

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

$$d^s_{+,\oplus}(\alpha, \beta) = 2^{-u} \sum_{k \in V_u} \delta(s(k + \alpha) \oplus s(k), \beta). \quad (5)$$

Також покладемо

$$\Delta^s_{\oplus,+} = \max_{\alpha, \beta \in V_u \setminus \{0\}} d^s_{\oplus,+}(\alpha, \beta), \quad (6)$$

і аналогічно визначимо

$$\Delta^s_{\oplus,\oplus}, \quad \Delta^s_{+,+} \text{ та } \Delta^s_{+,\oplus}. \quad (7)$$

Зауважимо, що імовірність диференціалу шифру та імовірність його диференціальної характеристики прямо пропорційна Δ^u, де Δ – один з параметрів (6) та (7), в залежності від операції у ключовому суматорі та від операції, відносно якої беруться вхідна та вихідна різниці. Показник степені залежить від відповідного індексу галуження та деяких інших параметрів шифру. Тому, збільшуючи імовірність раундового диференціалу, ми тим самим збільшуємо імовірність диференціалу та диференціальної характеристики всього шифру, тобто зменшуємо його стійкість до різницевого криптоаналізу. Загрози зменшення стійкості шифру можна спостерігати у наступних варіантах внесення змін.

Загроза 1. Некоректна заміна ключового суматора.

Варіант 1а. Відбувається заміна ключового суматора з операції побітового додавання на операцію модульного додавання.

Аргументом для такої заміни може бути помилкове обґрунтування: підвищення нелінійності шифру призведе до збільшення стійкості до різницевого криптоаналізу.

Потенційна загрозою у цьому варіанті є зменшення стійкості до цілочисельного або класичного різницевого криптоаналізу.

Умовою реалізації загрози є наявність у раундовій функції таких s-блоків, для яких

$$\Delta^s_{+,\oplus} > \Delta^s_{\oplus,\oplus} \quad (8)$$

або

$$\Delta^s_{+,+} > \Delta^s_{\oplus,+}. \quad (9)$$

Дійсно, згідно [19], після такої заміни ключового суматора максимальна імовірність раундового побітового диференціалу буде визначатись параметром $\Delta^s_{+,\oplus}$ замість $\Delta^s_{\oplus,\oplus}$, а імовірність раундового цілочисельного диференціалу – параметром $\Delta^s_{+,+}$ замість $\Delta^s_{\oplus,+}$.

З метою перевірки положень було проведено моделювання на комп'ютері, під час якого за методом бесповторного набору були сгенеровані конкретні значення s-блоків S_1 - S_{10} (зразки наведені на рис. 1, 2), що задовольняють умові (8).

В таблиці 1 наведені параметри $\Delta^s_{+,\oplus}$ та $\Delta^s_{\oplus,\oplus}$, що визначатимуть максимальну імовірність раундового побітового диференціалу для сгенерованих s-блоків.

Таблиця 1

Параметри s-блоків S_1 - S_{10}, що задовольняють умові (8)

s-блок	$\Delta^s_{+,\oplus}$	$\Delta^s_{\oplus,\oplus}$	s-блок	$\Delta^s_{+,\oplus}$	$\Delta^s_{\oplus,\oplus}$
S_1	0,04296875	0,0390625	S_2	0,04296875	0,0390625
S_3	0,04296875	0,0390625	S_4	0,04296875	0,0390625
S_5	0,04296875	0,0390625	S_6	0,04296875	0,0390625
S_7	0,04296875	0,0390625	S_8	0,04296875	0,0390625
S_9	0,04296875	0,0390625	S_{10}	0,04296875	0,0390625

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{11} - S_{20} (зразки наведені на рис. 3, 4), що задовольняють умові (9).

В таблиці 2 наведені обчислені їх параметри $\Delta^s_{+,+}$ та $\Delta^s_{\oplus,+}$, що визначатимуть імовірність раундового цілочисельного диференціалу.

B1	0D	F6	4B	AD	F3	D6	63	AC	FD	7A	EB	A1	C6	6C	06
B8	05	9B	7B	B0	18	45	A3	95	17	31	19	6D	73	59	83
DF	36	0B	71	41	68	C8	ED	26	21	B6	5A	4D	F4	E6	D5
B9	1C	09	44	12	D1	98	A4	CA	84	43	94	90	4C	C2	56
53	9E	54	6E	51	3A	23	D3	29	FB	10	3C	60	AF	9F	2E
CD	0C	82	46	91	27	99	DC	7D	FA	E4	74	5C	B5	BA	7C
4F	04	EF	8A	00	D0	2C	E9	81	F8	D7	BF	13	61	87	DA
4E	34	96	16	64	89	37	39	FF	6F	20	7F	B4	65	1A	F0
3D	24	C4	4A	A2	F1	42	DD	F2	EE	5B	8D	48	C5	50	B3
1D	E2	52	3B	C1	C3	B2	E8	BB	1B	1E	67	88	E1	57	CE
A0	69	35	A5	8B	0F	0A	1F	D8	78	38	B7	02	E0	2A	EC
79	72	AB	9A	AA	14	D9	62	5F	80	9C	C9	DB	BD	8E	E5
FE	D2	F7	A6	A9	C0	D4	32	77	15	3E	AE	28	CF	30	22
92	0E	9D	93	85	2F	6B	2B	5E	55	03	11	2D	F5	C7	6A
97	F9	49	E3	07	33	66	70	75	76	08	EA	BC	58	A7	CB
40	86	A8	7E	01	47	8C	FC	E7	DE	3F	5D	BE	8F	CC	25

3C	A9	95	E7	E5	4F	36	B8	3E	C1	B3	29	20	DC	F3	AB
6A	64	6E	85	D5	68	7F	87	CC	5C	80	E4	EB	93	BD	53
2A	81	50	7C	4D	CF	58	67	99	89	E2	3F	E6	CB	65	91
56	A8	42	1C	E1	A2	AC	5D	83	63	98	05	D7	B4	2B	61
C6	54	47	F1	D3	BC	9F	FD	7D	02	4C	FA	AD	F9	DF	0D
19	8E	A3	11	B0	FB	2F	07	B5	9C	23	9B	45	6B	00	94
D2	04	88	39	F5	E9	8F	1D	C2	EC	37	24	D6	3B	D0	35
51	C3	B2	21	1E	C9	C0	3A	48	13	0C	72	2E	40	43	BE
F0	82	74	34	A4	79	0A	4E	D1	7E	46	8A	52	59	26	09
BB	EA	DE	CE	ED	8D	15	A5	6F	C7	49	4B	E0	1F	25	BF
08	69	22	9E	2C	17	03	CA	77	8B	F6	FF	84	6C	BA	4A
F8	A6	73	30	92	0B	97	F2	12	B7	90	86	10	C8	27	E8
33	D8	1A	E3	06	01	31	AA	0F	A0	9A	16	66	A1	28	9D
0E	62	2D	EE	B6	60	70	57	FC	7A	6D	41	C4	5F	DA	71
7B	D9	8C	55	FE	B1	3D	5B	78	AF	CD	38	DB	32	C5	D4
44	DD	5E	96	B9	18	75	1B	14	A7	AE	EF	5A	76	F4	F7

Рис. 1. Значення S – блоків S_1 (зліва) та S_2

2A	A2	12	42	5E	1F	CA	2B	17	CE	3C	11	50	C0	CB	69
80	41	29	A7	06	87	DC	CD	DD	84	4C	EA	39	2F	34	58
81	0D	D8	6C	B4	4B	78	48	98	B2	AB	D9	43	B6	EC	25
F0	AE	F9	89	40	30	55	93	60	7A	AC	BC	F7	1A	8D	04
7B	F5	D4	0B	6F	0E	E9	B8	9D	45	BE	FD	F2	2D	B0	E2
96	D5	7C	90	B9	6E	18	FC	C9	82	00	22	DB	73	ED	64
E3	91	9E	71	24	26	4D	14	A8	19	36	0F	85	B3	03	B7
95	67	75	56	3A	AA	BF	3F	6D	0C	FB	23	A0	E6	3D	C7
10	BA	D2	BB	8A	C1	7D	F6	32	15	99	21	9C	B1	1B	05
61	EF	35	C8	44	F1	47	EB	38	63	C5	4E	E4	86	27	A1
BD	D1	01	52	09	70	F3	3E	FA	28	D3	3B	E0	C6	DA	2E
A6	F8	1E	02	D0	08	92	5B	FF	46	7F	59	CC	8C	D6	8F
F4	C2	13	1C	CF	16	9F	AF	5A	6A	D7	7E	4A	AD	57	5F
54	8E	A9	9A	EE	68	77	E8	62	94	97	88	DF	FE	2C	49
31	51	74	A4	20	A5	8B	76	53	9B	07	72	E1	0A	33	37
C4	5D	A3	5C	4F	C3	65	1D	79	DE	6B	E7	B5	66	E5	83

1B	41	C8	03	A2	77	34	42	68	F6	E4	8A	44	45	5D	40
6F	9B	5C	C3	E5	11	23	83	6C	E8	0B	74	B5	9A	C9	29
D0	54	13	FE	36	3B	6D	E9	71	BB	19	8D	4A	1A	DE	05
2C	F5	7E	4C	3A	B2	7B	50	3C	12	69	DB	62	38	2D	27
20	9C	F0	26	60	B7	14	00	33	CA	18	D6	B6	E6	1D	09
C2	E0	06	39	0C	02	78	63	92	4E	C4	3E	6A	B9	CC	DF
21	F1	C7	D9	D1	F9	0F	A5	9E	7D	73	37	0D	0E	5E	A0
A4	79	85	A8	87	CE	1F	16	E3	B3	58	89	BF	2B	E1	BC
28	81	52	7F	D2	56	D7	49	6E	82	72	25	8E	51	E7	FC
53	C6	8C	2E	7A	70	96	EF	65	A1	4D	98	DA	6B	CF	C0
BD	F7	EB	AD	CD	8F	BA	46	B1	80	59	3F	9D	AE	4B	07
F4	17	FA	2F	99	94	AC	10	84	43	B0	AA	97	FF	48	90
C5	08	C1	1E	35	64	F8	A6	F3	7C	8B	5B	A3	AB	CB	B4
88	24	B8	61	76	FD	2A	31	75	66	95	A9	D3	1C	AF	DC
93	22	3D	47	F2	32	5F	0A	D8	04	D4	15	4F	01	DD	67
BE	55	EC	5A	E2	9F	30	86	FB	D5	EA	A7	ED	91	EE	57

Рис. 2. Значення S – блоків S_3 (зліва) та S_4

99	15	E4	56	8C	AC	7B	95	6E	40	84	35	BB	68	FD	9D
A5	DD	B4	3B	D3	C6	6C	6F	CE	41	61	F5	25	0B	1E	CC
7E	54	78	B2	3C	AA	7F	5C	55	0D	02	CB	A6	B6	27	2B
F8	59	88	39	2D	C3	7D	4D	A8	89	36	EF	DA	EC	47	DB
7C	1D	DF	5F	5D	A1	23	57	10	FF	D0	00	11	BE	DE	B7
EA	07	18	69	4B	94	E8	C4	DC	29	67	C9	97	86	ED	32
D1	21	2A	8D	9A	8B	20	74	3E	52	5E	03	51	34	C2	0E
0F	C5	43	1F	D8	E7	D9	05	76	E5	B3	7A	B9	72	63	D6
4A	AF	FA	F3	5A	A3	2E	CD	65	F0	14	5B	F1	FC	A0	77
60	AE	66	C8	30	62	C0	BA	6D	08	37	33	80	D5	64	70
F9	1B	9C	53	82	9B	D7	50	42	CF	45	8A	31	06	58	48
91	BF	4E	BD	F6	E9	CA	F4	C7	EE	13	2C	46	6B	0A	F2
3A	A2	17	D4	44	E2	A9	AD	1A	A4	E1	92	24	BC	38	04
87	71	B8	1C	90	3F	19	D2	22	8E	E0	98	2F	6A	09	C1
93	96	EB	75	01	73	8F	79	9E	28	26	A7	B0	0C	F7	3D
49	E6	4F	12	9F	FE	B1	4C	81	AB	FB	E3	85	B5	83	16

27	4E	5F	89	3B	11	62	0F	23	B3	F2	E1	D8	DE	71	43
8E	E4	78	EA	FB	C2	E2	D7	60	0C	92	D2	91	D4	9C	A5
51	E6	54	1F	44	B8	84	82	9E	FC	C6	3F	56	1E	20	8A
E8	8D	AD	9F	B6	34	4D	31	28	AB	ED	D3	57	C9	8B	B9
4F	A1	CC	AE	35	F6	08	0B	F3	6C	CD	61	22	EE	A8	8C
83	DA	CB	C1	15	58	D1	EB	87	A3	21	7E	6B	97	4B	FA
B1	41	F4	F8	A7	C7	C8	4C	DB	25	09	3D	66	6A	07	C4
AC	67	F1	29	18	01	A0	72	2A	C0	C5	BD	DD	13	53	88
93	A2	F5	C3	1C	5E	B5	FE	1A	37	74	55	A9	5A	E5	BE
52	B0	1B	68	EC	64	04	45	CF	7B	38	19	2E	47	9D	DC
1D	99	6F	14	10	90	E3	F0	95	2F	7D	12	75	7A	39	F9
03	FD	26	3A	98	7C	F7	59	96	24	70	33	30	5C	46	40
81	D6	94	63	79	E0	B2	48	5B	06	5D	E9	50	BB	9A	8F
FF	76	CA	3C	32	BC	2B	A4	B4	AF	9B	EF	2C	DF	6D	6E
B7	00	E7	3E	77	0E	0D	CE	2D	D9	49	73	16	86	02	65
0A	7F	A6	42	80	AA	BA	BF	85	D5	D0	4A	05	69	17	36

Рис. 3. Значення S – блоків S_{11} (зліва) та S_{12}

73	27	92	DE	17	D7	6F	A4	21	FA	F0	1F	3A	71	78	F5
D9	23	34	0B	C5	B7	76	C7	CF	91	4B	99	AA	88	9E	DF
82	8F	7C	96	2F	35	16	E1	5C	7D	14	AB	B0	E8	F7	0A
98	F6	80	B1	ED	D6	8E	60	08	F9	8D	19	24	DC	A9	01
E3	EA	45	E0	B9	6C	F3	3D	2B	72	C6	FD	EE	8B	29	2A
E6	BF	77	D2	1A	51	A8	FF	31	44	38	6D	95	1B	48	47
37	E5	AD	74	86	FB	36	F2	2D	70	EC	46	A1	54	5B	90
05	39	D8	87	4A	A7	11	75	62	DD	6A	A5	E9	0F	12	58
B4	CE	61	79	40	A2	D3	4D	B2	69	94	97	E7	3F	DB	07
28	AF	EB	CC	CA	64	59	8A	89	C9	26	43	65	84	D5	2C
B6	42	9C	E4	BC	22	AE	5D	30	BD	DA	FC	15	BA	57	9D
BB	83	53	A3	02	13	93	85	C1	9F	1C	3E	C2	56	63	7F
1D	06	C4	4E	00	68	CB	5E	EF	10	C0	2E	55	52	4C	04
B5	4F	81	D4	8C	1E	D0	7A	25	C8	7B	03	C3	5A	D1	41
66	09	6B	49	A6	50	3C	33	6E	0E	F1	7E	F8	67	32	9A
E2	F4	3B	BE	CD	0D	FE	9B	18	0C	B8	B3	AC	5F	20	A0

1D	48	02	BA	DD	AE	C7	3E	08	21	72	35	06	15	2C	E1
2B	5F	94	0A	78	C0	BC	99	19	D5	1A	FF	9D	69	03	85
77	DF	8A	FB	55	74	36	46	14	47	DA	4B	F8	A1	D3	82
D2	5A	CF	61	D1	2F	E6	BD	84	34	24	D0	11	0C	81	59
86	12	1B	EC	2D	27	9F	07	EF	8E	33	F3	50	95	39	76
41	16	66	B0	6A	F1	AF	52	C6	71	F5	CC	B2	A7	8F	FA
26	ED	7F	DC	7B	CA	A2	CD	37	AA	C3	9A	DE	A4	B8	D9
BB	45	54	F4	7E	5E	3B	B1	4F	D8	CB	6C	EE	0D	80	E8
44	13	DB	67	00	B6	6B	7C	F7	E4	1E	09	05	0E	A5	FD
89	EA	7D	8C	38	9C	A3	E3	2A	04	4C	29	9B	C2	90	C8
01	A9	F2	0B	68	1C	5D	FC	FE	30	32	3D	17	91	D4	C5
83	70	92	28	18	B5	43	49	2E	3A	98	F6	3F	3C	5B	AB
C1	96	9E	4D	23	87	25	CE	BF	10	79	73	6D	B4	51	A6
6E	65	C9	1F	58	5C	B9	8B	D6	42	6F	E9	D7	57	B3	8D
F9	31	88	0F	63	4E	B7	A8	60	A0	56	75	97	7A	53	BE
F0	93	E7	64	E0	4A	C4	E5	AC	EB	20	62	22	40	E2	AD

Рис. 4. Значення S – блоків S_{13} (зліва) та S_{14}

Таблиця 2

Параметри s-блоків S_{11} - S_{20}, що задовольняють умові (9)

s-блок	$\Delta^s_{+,+}$	$\Delta^s_{\oplus,+}$	s-блок	$\Delta^s_{+,+}$	$\Delta^s_{\oplus,+}$
S_{11}	0,03515625	0,03125	S_{12}	0,03125	0,0234375
S_{13}	0,03125	0,0234375	S_{14}	0,03515625	0,03125
S_{15}	0,03125	0,02734375	S_{16}	0,03125	0,02734375
S_{17}	0,03125	0,02734375	S_{18}	0,03515625	0,02734375
S_{19}	0,03125	0,02734375	S_{20}	0,03125	0,02734375

Варіант 1б. Передбачає заміну ключового суматора з операції модульного додавання на операцію побітового додавання.

У разі малої обчислювальної потужності процесора проектантам для збільшення швидкодії процедур криптографічного перетворення, враховуючи достатню нелінійність s-блоків, уявляється є зайвим внесення нелінійності модульного додавання, до того ж суттєво уповільнюючим процес шифрування.

Потенційною загроза у цьому варіанті є зменшення стійкості до цілочисельного або класичного різницевого криптоаналізу.

Умовою реалізації загрози є наявність у раундовій функції таких s-блоків, для яких

$$\Delta^s_{\oplus,\oplus} > \Delta^s_{+,\oplus} \quad (10)$$

або

$$\Delta^s_{\oplus,+} > \Delta^s_{+,+}. \quad (11)$$

Обгрунтування: згідно [19], після такої заміни ключового суматора максимальна імовірність раундового побітового диференціалу буде визначатись параметром $\Delta^s_{\oplus,\oplus}$ замість $\Delta^s_{+,\oplus}$, а імовірність раундового цілочисельного диференціалу – параметром $\Delta^s_{\oplus,+}$ замість $\Delta^s_{+,+}$.

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{21} - S_{30} (зразки наведені на рис. 5, 6), що задовольняють умові (10), а в таблиці 3 наведені їх параметри $\Delta^s_{\oplus,\oplus}$ та $\Delta^s_{+,\oplus}$ та, що визначатимуть максимальну імовірність раундового побітового диференціалу.

```
2B 4C 58 CB B9 D7 FD E4 5A F3 F1 07 ED B4 53 3A    BB 07 37 F3 95 FC EC A1 FE 0E F1 32 77 E2 D6 C0
8A 0D 19 DC 65 F7 4E CD BC DA 9C C9 5D 42 75 7D    81 06 39 3F 5C AC 53 1D 5E 03 CE 0C 8E 51 19 63
93 14 2D AD 54 EA 57 25 46 51 67 FF 82 41 8E FA    08 40 AA 58 BC 4C C6 E5 D9 D8 97 DF BE B7 29 1F
56 1C C8 3E 52 DB 5B 7E D6 61 0C C2 77 D4 E3 A8    27 8F 6A EE E3 4A 4B AB 2A 73 B6 A7 FB C2 7D F8
AF 28 C3 59 E2 50 4A 43 B7 AA B0 02 32 94 87 89    E7 13 35 A8 D2 9C 66 A9 E0 EF 67 A4 52 61 17 24
9A D2 A3 34 2C 63 2E C5 30 60 36 9D 2A 6A 39 74    18 93 45 05 3A B5 36 CC 12 1A FD 76 8C 56 D0 00
11 C7 1A CF 9F EE 99 81 7A D8 5C C0 BB 09 A1 9E    F0 F5 F9 5A FF B0 AF B2 C5 55 31 C3 7C E9 E6 2E
C4 3B 5F 91 1F FC 96 D0 BD 8D D3 00 10 E1 A7 DF    9D 9F DB 3D C7 44 92 6D 4D 78 CB 47 20 0B 1B 72
8C 12 2F 16 26 A2 F4 1E 33 A6 08 6B F6 35 F2 B5    79 CF 4E A0 B9 7B 54 A2 B1 34 D1 14 57 26 43 E8
70 3F 6F F5 CC 38 CE FE 3D 80 97 A5 31 98 A0 01    25 91 C8 87 94 4F EA D5 3E AD 30 42 B8 2C B4 C1
8F 55 E0 C1 64 0E 48 44 AB B8 1D 40 4B B6 73 D9    E4 7E 9E 2D 49 89 15 23 7F 80 CD D7 DD F6 85 28
83 69 0F 06 72 27 0B 7B 0A FB 6D A4 8B 4D 92 15    33 F4 BD 09 DE 9B D4 74 2B 0F FA 65 5F 59 84 41
88 E8 86 AC 78 03 E9 BE 85 04 18 49 62 45 BF D1    7A 71 EB 3C 60 A3 BA E1 6F 10 1E 98 6E DA 62 70
84 29 47 EB 6E 23 CA F9 66 C6 20 F8 21 76 3C 17    02 69 A6 BF A5 82 88 50 3B 16 C9 04 01 CA 8B 64
13 90 DD BA 37 F0 24 5E 7C B3 7F E6 4F 1B AE A9    5B 1C 90 F2 46 11 21 5D 8D 6B 9A F7 ED 0D 48 B3
E7 DE 6C D5 E5 05 EC 71 EF 68 22 B2 79 B1 95 9B    AE 0A C4 2F 8A DC 68 75 86 96 99 38 83 22 D3 6C
```

Рис. 5. Значення S – блоків S_{21} (зліва) та S_{22}

```
67 E0 61 D6 FC 35 24 08 1D 9F 8F A4 79 21 37 9A    FF 35 DC 04 9C 2A FB 6F 12 E5 47 C3 C2 0D 3A 01
71 3D F9 1F A1 EA 4A D3 9C 1E B0 50 B8 23 F7 80    BD FC A6 59 AC 09 D9 C0 D7 82 7A 92 9B 62 EF CD
5C 53 5B 56 C5 2A D0 CD AC EB 3E E6 0F 15 28 95    B1 21 7E 49 83 24 66 52 BB 3F 1F B0 44 D2 8C AA
04 2E 3A C6 7A 5A 84 31 C2 1B 10 86 AA 85 38 92    E2 E3 AF 43 F9 C4 CE 30 8A FD 07 31 E1 8F 27 CF
39 EC 9B 3F C8 4C 00 88 A8 90 82 2B 43 70 7C 7D    F4 74 0F 70 81 99 61 A2 F2 CA 9F 73 4C A3 41 B9
B4 AB F0 B9 E1 E8 D5 12 BD 93 BC B1 8A FE FB F3    05 02 00 19 B2 84 68 F0 77 B5 A1 87 D6 96 E8 BE
F5 D4 77 CA 91 BB 9D 8E 7F DA C9 D9 11 0D 57 6F    36 5E 4B 76 9E 79 B4 18 F3 7C A0 C1 32 69 A5 7F
8B 64 3C A2 68 F4 D8 EF B3 76 44 BE DD E5 07 01    9D E4 88 AD 13 53 D8 20 6A 2B 2D 80 39 4E 37 0E
DF 40 5D 62 0E ED E4 6E 75 E3 20 2F 9E EE F2 06    2E 3E F5 94 B7 15 42 11 22 28 FE A4 5C 51 2C 75
46 2D FD C3 42 98 89 09 72 74 D1 C1 1C B2 AD 59    4A 6B 33 E9 1A 1C 6D C7 3C BC 60 0A E7 DA 1D 78
6C 87 4F DC 16 6D C7 32 02 4D DE 2C 5F A6 F8 E9    E6 98 2F 71 50 E0 03 08 85 F6 C6 8B D0 64 BA F1
22 CF 97 7B 4E B7 D2 27 FF 03 E7 55 B5 BA 0C 25    5B 40 6E EE 10 14 4D 6C DF 86 FA 4F DE 23 0B EA
B6 52 1A F6 51 0A 6A 48 45 C0 83 73 58 C4 41 47    A9 5D 7B 55 C5 57 F8 ED D4 9A C9 48 46 06 3B D5
33 8C 78 D7 49 13 AF A3 4B 36 5E 96 DB A0 6B 30    CB 34 A7 DD 56 90 A8 38 1E 91 29 D1 AE 63 97 3D
99 F1 CC AE A5 0B 14 FA CB 69 05 26 18 3B 63 66    B8 5F 25 26 93 AB 8D EB B6 65 B3 1B 16 72 67 CC
54 60 17 29 19 34 81 CE 7E A7 94 E2 A9 BF 8D 65    F7 89 95 0C 45 17 8E 54 7D C8 58 BF EC DB 5A D3
```

Рис. 6. Значення S – блоків S_{23} (зліва) та S_{24}

Таблиця 3

Параметри s-блоків S_{21} - S_{30}, що задовольняють умові (10)

s-блок	$\Delta^s_{\oplus,\oplus}$	$\Delta^s_{+,\oplus}$	s-блок	$\Delta^s_{\oplus,\oplus}$	$\Delta^s_{+,\oplus}$
S_{21}	0,046875	0,03125	S_{22}	0,046875	0,03125
S_{23}	0,0390625	0,03125	S_{24}	0,0390625	0,03125
S_{25}	0,046875	0,03125	S_{26}	0,046875	0,02734375
S_{27}	0,046875	0,02734375	S_{28}	0,046875	0,02734375
S_{29}	0,046875	0,02734375	S_{30}	0,046875	0,03125

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{31} - S_{40} (зразки наведені на рис. 7, 8), що задовольняють умові (11), а в таблиці 4 наведені параметри $\Delta^s_{\oplus,+}$ та $\Delta^s_{+,+}$, що визначатимуть імовірність раундового цілочисельного диференціалу.

FC	01	BB	11	5F	0D	F7	87	96	1C	DA	CA	90	02	E7	A8
37	8B	D3	5A	59	46	3A	3F	72	32	CE	C5	93	8D	FB	41
22	4E	10	4A	D6	6A	C7	0E	B4	CF	DD	DF	76	CD	EB	BD
2A	27	13	25	18	EA	BA	9E	69	A9	F3	8F	99	05	E0	EE
66	B2	31	14	75	45	E2	0C	92	CC	9D	38	91	84	A0	55
68	8C	A4	4D	40	8A	88	A5	4C	AD	E5	80	86	D9	23	09
D0	C6	FE	C1	AC	D2	6D	65	C4	F5	B1	FA	3C	FF	24	36
D7	21	7D	07	B6	A2	C2	30	E9	3B	7F	AA	3E	97	79	71
7B	F0	E4	62	52	12	29	28	06	0F	20	95	04	AB	0B	4F
B9	4B	CB	7E	78	5D	D8	1E	16	E1	D5	EF	9C	E6	7A	67
73	B5	89	3D	34	35	AE	49	33	54	DC	03	58	C0	DE	2E
00	42	48	19	6F	63	85	77	F4	B7	56	81	6C	D4	26	B8
2F	F2	1D	2C	57	A1	74	F6	83	C8	A6	44	AF	8E	1B	A3
C3	5E	1A	BE	53	C9	BF	7C	D1	47	2D	51	B0	E3	70	9A
43	39	F9	A7	5B	82	17	F1	1F	60	2B	B3	50	DB	0A	9F
98	ED	61	F8	E8	5C	94	EC	6E	64	15	9B	08	6B	FD	BC

88	05	E8	52	53	66	F5	34	29	5B	C9	35	B5	E3	F7	06
1A	71	AD	02	92	E4	7B	43	2E	81	5A	A3	12	3F	A5	4B
28	41	2D	89	DF	BF	74	BE	C1	27	7A	20	3D	C5	97	D4
45	32	2A	5D	6A	CC	72	9B	49	94	3E	1F	B9	A6	87	E9
0A	2B	A9	CE	7D	ED	83	FD	21	57	3A	31	58	15	80	36
2C	38	75	98	4A	E1	54	04	AB	A2	69	11	BA	3C	09	84
7C	73	8D	07	78	B7	4F	B4	7F	D8	61	14	F6	BB	D2	47
77	0F	16	95	63	08	82	50	F4	EE	C4	DC	EF	1D	65	00
8C	D9	6D	6E	48	DA	0D	46	D6	B1	86	44	22	9D	F0	99
10	40	E5	1E	8B	F2	5C	A1	19	01	3B	93	BC	55	70	91
E6	1B	60	DD	62	EA	F3	B6	BD	96	51	E7	9E	03	0C	8A
67	37	6F	7E	18	C7	90	D5	8E	A8	33	56	6B	D1	68	B3
5F	AA	C8	CD	39	D0	9A	64	5E	26	4D	23	A4	9C	C3	25
30	D3	EB	76	0B	13	FE	2F	CA	AF	59	C0	B0	DE	4C	E0
FC	1C	CF	A0	AE	DB	F9	EC	B2	AC	FB	24	B8	17	85	C6
9F	FF	E2	F8	79	F1	D7	A7	42	6C	FA	CB	0E	C2	8F	4E

Рис. 7. Значення S – блоків S_{31} (зліва) та S_{32}

AA	F6	FF	52	A6	B3	9E	70	D6	81	12	00	4B	6D	DC	72
10	8D	18	F7	C5	AD	83	68	A8	FE	A7	3A	30	8F	99	A2
71	21	1D	17	A9	56	5F	A0	E9	2B	20	07	5D	55	4E	FA
1B	E5	B8	7E	02	1F	82	4A	75	BD	57	0C	BA	3E	AE	FB
76	94	EB	D5	C2	77	B6	38	16	EE	62	23	42	09	59	53
19	98	DB	27	B7	DE	22	B0	CA	F9	EA	31	05	11	50	5B
7A	28	B5	A1	92	E7	29	46	B4	33	25	D8	0B	49	85	6A
7F	EF	13	2D	54	A3	36	D7	58	8C	73	CF	35	BC	66	48
7D	BE	DF	80	E2	D3	F1	E1	F5	C7	74	69	91	E8	5A	1E
EC	34	E6	14	B9	C8	06	A5	60	08	1C	8B	9A	79	CC	CB
2C	86	6E	37	7C	AC	0E	93	0D	FC	84	D1	45	24	6B	CE
4D	B2	04	9F	61	CD	8A	C1	88	5C	F4	A4	C0	AF	26	4C
ED	39	44	8E	1A	2A	F8	F3	D9	AB	2E	BF	47	41	5E	97
C3	9B	C4	BB	96	6F	D4	DA	03	6C	B1	95	E0	4F	F0	0A
15	3F	E4	01	51	63	C9	40	D0	3B	64	87	43	78	9D	DD
3D	FD	7B	D2	67	89	65	3C	2F	F2	32	E3	90	9C	0F	C6

21	D4	1D	D9	7A	7B	FE	68	8A	8C	3B	1A	95	45	82	E7
36	49	CF	EE	05	75	C6	EA	2D	FC	4E	D0	46	6B	3C	E6
81	62	B0	61	35	66	4B	F0	67	A7	37	57	E2	E1	EF	65
BE	4D	8E	F2	07	69	B2	DF	5F	6C	71	0E	FA	41	04	43
48	BB	E4	27	9F	93	E8	AC	98	40	08	94	F3	54	03	1E
9B	EC	8B	F1	56	53	14	01	20	0C	2C	F5	BD	30	84	C9
10	5D	2F	6F	92	23	78	A9	26	52	F9	15	C7	72	8F	A1
D2	51	24	C3	89	B4	5B	87	B7	A3	CB	17	C0	55	FF	25
BC	29	3F	9C	BA	13	12	31	F8	9E	D3	44	E0	AA	AE	91
79	D8	39	F4	B1	E3	1C	2E	38	DD	88	90	19	22	F7	6E
A0	0D	99	74	AD	34	BF	C5	1B	5A	18	DB	3E	33	0B	32
B6	50	F6	83	B8	C2	5C	A4	59	85	64	4C	DE	47	9A	3D
C4	C1	8D	CD	DC	DA	5E	A2	D6	73	77	0F	86	CC	B5	6D
B9	A5	0A	CE	09	70	4A	63	58	C8	97	4F	9D	3A	E9	FB
02	06	1F	EB	7D	D7	7C	76	ED	FD	A8	D1	42	00	D5	28
E5	2A	6A	16	7E	96	80	11	AB	CA	A6	2B	60	7F	B3	AF

Рис. 8. Значення S – блоків S_{33} (зліва) та S_{34}

Таблиця 4

Параметри s-блоків S_{31} - S_{40}, що задовольняють умові (11)

s-блок	$\Delta^{s}_{\oplus,+}$	$\Delta^{s}_{+,+}$	s-блок	$\Delta^{s}_{\oplus,+}$	$\Delta^{s}_{+,+}$
S_{31}	0,03125	0,02734375	S_{32}	0,03125	0,02734375
S_{33}	0,03125	0,02734375	S_{34}	0,03515625	0,0234375
S_{35}	0,02734375	0,0234375	S_{36}	0,03125	0,02734375
S_{37}	0,03125	0,0234375	S_{38}	0,03125	0,02734375
S_{39}	0,02734375	0,0234375	S_{40}	0,03125	0,02734375

Загроза 2. Некоректна заміна s-блоків.

Відбувається заміна s-блоків з метою удосконалення шифру.

У цьому випадку метою заміни (реальною або замаскованою) є підвищення стійкості до побітового різницевого криптоаналізу.

Потенційною загрозою цього варіанту є зменшення стійкості до цілочисельного різницевого криптоаналізу.

Умовою реалізації загрози є наявність такого s-блоку s_1 у раундовій функції шифру та існування такого s-блоку s_2, для яких одночасно виконуються наступні умови:

якщо у ключовому суматорі шифру реалізовано операцію побітового додавання, то

$$\Delta^{s_1}_{\oplus,+} < \Delta^{s_2}_{\oplus,+},\ \Delta^{s_1}_{\oplus,\oplus} > \Delta^{s_2}_{\oplus,\oplus} \text{ та } \Delta^{s_1}_{\oplus,\oplus} < \Delta^{s_2}_{\oplus,+}; \quad (12)$$

якщо у ключовому суматорі шифру реалізовано операцію модульного додавання, то

$$\Delta^{s_1}_{+,+} < \Delta^{s_2}_{+,+},\ \Delta^{s_1}_{+,\oplus} > \Delta^{s_2}_{+,\oplus} \text{ та } \Delta^{s_1}_{+,\oplus} < \Delta^{s_2}_{+,+}. \quad (13)$$

Обґрунтування: згідно [19], максимальна імовірність раундового цілочисельного диференціалу після заміни s-блоку S_1 на s-блок S_2 буде визначатись параметром $\Delta^{s_2}_{\oplus,+}$ у першому випадку і $\Delta^{s_2}_{+,+}$ у другому випадку, і цей параметр буде більшим, ніж відповідні параметри, залежні від s_1, як для цілочисельного, так і для класичного диференціалу.

Для проведення експериментальних досліджень були обрані s-блоки, що наведені на рис. 9-13.

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

$\Delta^{s_1}_{\oplus,\oplus} = 0{,}015625,\ \Delta^{s_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{s_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{s_1}_{+,+} = 0{,}02734375$

Рис. 9. S-блок для алгоритму AES (Federal Information Processing Standards Publication 197)

```
A8 43 5F 06 6B 75 6C 59 71 DF 87 95 17 F0 D8 09
6D F3 1D CB C9 4D 2C AF 79 E0 97 FD 6F 4B 45 39
3E DD A3 4F B4 B6 9A 0E 1F BF 15 E1 49 D2 93 C6
92 72 9E 61 D1 63 FA EE F4 19 D5 AD 58 A4 BB A1
DC F2 83 37 42 E4 7A 32 9C CC AB 4A 8F 6E 04 27
2E E7 E2 5A 96 16 23 2B C2 65 66 0F BC A9 47 41
34 48 FC B7 6A 88 A5 53 86 F9 5B DB 38 7B C3 1E
22 33 24 28 36 C7 B2 3B 8E 77 BA F5 14 9F 08 55
9B 4C FE 60 5C DA 18 46 CD 7D 21 B0 3F 1B 89 FF
EB 84 69 3A 9D D7 D3 70 67 40 B5 DE 5D 30 91 B1
78 11 01 E5 00 68 98 A0 C5 02 A6 74 2D 0B A2 76
B3 BE CE BD AE E9 8A 31 1C EC F1 99 94 AA F6 26
2F EF E8 8C 35 03 D4 7F FB 05 C1 5E 90 20 3D 82
F7 EA 0A 0D 7E F8 50 1A C4 07 57 B8 3C 62 E3 C8
AC 52 64 10 D0 D9 13 0C 12 29 51 B9 CF D6 73 8D
81 54 C0 ED 4E 44 A7 2A 85 25 E6 CA 7C 8B 56 80
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{S_1}_{+,\oplus} = 0{,}0234375,\ \Delta^{S_1}_{+,+} = 0{,}03125$

Рис. 10. S-блок №1 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
CE BB EB 92 EA CB 13 C1 E9 3A D6 B2 D2 90 17 F8
42 15 56 B4 65 1C 88 43 C5 5C 36 BA F5 57 67 8D
31 F6 64 58 9E F4 22 AA 75 0F 02 B1 DF 6D 73 4D
7C 26 2E F7 08 5D 44 3E 9F 14 C8 AE 54 10 D8 BC
1A 6B 69 F3 BD 33 AB FA D1 9B 68 4E 16 95 91 EE
4C 63 8E 5B CC 3C 19 A1 81 49 7B D9 6F 37 60 CA
E7 2B 48 FD 96 45 FC 41 12 0D 79 E5 89 8C E3 20
30 DC B7 6C 4A B5 3F 97 D4 62 2D 06 A4 A5 83 5F
2A DA C9 00 7E A2 55 BF 11 D5 9C CF 0E 0A 3D 51
7D 93 1B FE C4 47 09 86 0B 8F 9D 6A 07 B9 B0 98
18 32 71 4B EF 3B 70 A0 E4 40 FF C3 A9 E6 78 F9
8B 46 80 1E 38 E1 B8 A8 E0 0C 23 76 1D 25 24 05
F1 6E 94 28 9A 84 E8 A3 4F 77 D3 85 E2 52 F2 82
50 7A 2F 74 53 B3 61 AF 39 35 DE CD 1F 99 AC AD
72 2C DD D0 87 BE 5E A6 EC 04 C6 03 34 FB DB 59
B6 C2 01 F0 5A ED A7 66 21 7F 8A 27 C7 C0 29 D7
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}0234375$

Рис. 11. S-блок №2 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

Тут в якості блоку S_1 може бути будь-який з s-блоків (№№ 1 – 4) алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014 та AES.

Під час проведення експериментальних досліджень не вдалося отримати жодного s-блоку, який задовольняє умові (12).

В той же час існує досить багато s-блоків, що задовольняють умові (13). Зокрема, цій умові задовольняють майже всі s-блоки (крім s-блок №1) алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014.

На рис. 14, 15 наведені конкретні значення s-блоків, що задовольняють умові (13), а в таблиці 3 наведені значення відповідних параметрів $\Delta^{S}_{+,\oplus}$ та $\Delta^{S}_{+,+}$.

```
93 D9 9A B5 98 22 45 FC BA 6A DF 02 9F DC 51 59
4A 17 2B C2 94 F4 BB A3 62 E4 71 D4 CD 70 16 E1
49 3C C0 D8 5C 9B AD 85 53 A1 7A C8 2D E0 D1 72
A6 2C C4 E3 76 78 B7 B4 09 3B 0E 41 4C DE B2 90
25 A5 D7 03 11 00 C3 2E 92 EF 4E 12 9D 7D CB 35
10 D5 4F 9E 4D A9 55 C6 D0 7B 18 97 D3 36 E6 48
56 81 8F 77 CC 9C B9 E2 AC B8 2F 15 A4 7C DA 38
1E 0B 05 D6 14 6E 6C 7E 66 FD B1 E5 60 AF 5E 33
87 C9 F0 5D 6D 3F 88 8D C7 F7 1D E9 EC ED 80 29
27 CF 99 A8 50 0F 37 24 28 30 95 D2 3E 5B 40 83
B3 69 57 1F 07 1C 8A BC 20 EB CE 8E AB EE 31 A2
73 F9 CA 3A 1A FB 0D C1 FE FA F2 6F BD 96 DD 43
52 B6 08 F3 AE BE 19 89 32 26 B0 EA 4B 64 84 82
6B F5 79 BF 01 5F 75 63 1B 23 3D 68 2A 65 E8 91
F6 FF 13 58 F1 47 0A 7F C5 A7 E7 61 5A 06 46 44
42 04 A0 DB 39 86 54 AA 8C 34 21 8B F8 0C 74 67
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}02734375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}02734375$

Рис. 12. S-блок №3 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
68 8D CA 4D 73 4B 4E 2A D4 52 26 B3 54 1E 19 1F
22 03 46 3D 2D 4A 53 83 13 8A B7 D5 25 79 F5 BD
58 2F 0D 02 ED 51 9E 11 F2 3E 55 5E D1 16 3C 66
70 5D F3 45 40 CC E8 94 56 08 CE 1A 3A D2 E1 DF
B5 38 6E 0E E5 F4 F9 86 E9 4F D6 85 23 CF 32 99
31 14 AE EE C8 48 D3 30 A1 92 41 B1 18 C4 2C 71
72 44 15 FD 37 BE 5F AA 9B 88 D8 AB 89 9C FA 60
EA BC 62 0C 24 A6 A8 EC 67 20 DB 7C 28 DD AC 5B
34 7E 10 F1 7B 8F 63 A0 05 9A 43 77 21 BF 27 09
C3 9F B6 D7 29 C2 EB C0 A4 8B 8C 1D FB FF C1 B2
97 2E F8 65 F6 75 07 04 49 33 E4 D9 B9 D0 42 C7
6C 90 00 8E 6F 50 01 C5 DA 47 3F CD 69 A2 E2 7A
A7 C6 93 0F 0A 06 E6 2B 96 A3 1C AF 6A 12 84 39
E7 B0 82 F7 FE 9D 87 5C 81 35 DE B4 A5 FC 80 EF
CB BB 6B 76 BA 5A 7D 78 0B 95 E3 AD 74 98 3B 36
64 6D DC F0 59 A9 4C 17 7F 91 B8 C9 57 1B E0 61
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}02734375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}02734375$

Рис. 13. S-блок №4 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
1B 95 9E 90 2A 26 FF F4 CE C2 7A 6E 75 DF C4 B5
5B 50 19 EB 4D 7C 1C 5E B6 7B ED 3A 1F B9 0E 64
CA A5 87 30 A4 01 92 12 1E 10 BE 2D 05 00 58 29
36 78 98 DE 11 70 AD 06 37 4E E0 07 65 34 EA D9
E5 97 16 35 CB 39 99 6C 8B 0C B0 B4 E4 03 A3 74
AA 24 C9 46 E3 B1 EC 18 BF 48 A0 86 BB D8 BD 42
C1 51 4A 69 2F 47 31 73 F9 A7 89 C0 A6 AC 2C A1
8A D3 17 AF AB 57 27 EF 5D F5 0F 2E 22 25 55 C6
52 20 A8 60 62 E7 CC 68 33 80 D6 28 7F AE B7 8F
82 D2 09 63 9D 14 4F 4B 96 7D D1 7E FB EE F8 76
BA D5 53 94 3F DD CF 9B 85 8C C7 1A 93 FA 3B 56
43 1D 6A D7 9A FC F0 88 38 D4 81 F3 54 F6 61 B3
9F B2 49 0B 21 3D 6B F1 59 C8 72 E8 F2 41 FE E2
DA 4C 9C 08 E9 91 5A 2B 44 A2 83 79 02 6D 23 FD
DC E1 77 DB 32 0D 5F 45 3E 6F 40 C3 B8 BC 66 3C
04 C5 8D D0 E6 A9 0A 67 84 8E CD 5C F7 13 71 15
```

```
9C 34 98 44 8B 45 8D 49 F6 46 04 CB FB B3 08 C5
43 EA 38 AB A7 E5 4A CA F7 5F B6 B1 CC D9 DB 02
CF 5C 75 BD 16 83 54 7B 14 73 36 4E 33 68 C3 26
01 3E A5 FE E0 94 C8 BF 37 B7 FA F1 FC 95 5B AD
15 7F C4 BB 52 11 5D 97 27 86 74 A6 B4 09 96 F4
20 07 3D 67 9A E9 5E AC FF 99 6B 1A 0E 17 D8 8F
61 30 10 7A 3B C1 D0 03 00 AF D6 BC D2 9B 79 CE
AE DC 40 32 DF A1 EF 41 66 6A 7E D4 B8 1E B2 C6
2B 3C 0F 84 9D D5 06 62 4F A3 F9 0D C7 93 ED 8C
B0 71 F5 63 48 F3 88 DD 23 EE 0B DA E8 7D 4B 22
1F 5A 31 4D EC 76 70 77 BE E4 A0 F0 69 65 57 13
DE 82 78 D1 72 C9 CD 05 12 D3 E3 47 FD E2 EB 60
0C 0A B5 1C 7C 80 2F 28 53 2E 8E 90 19 81 9F 50
9E E1 55 A8 42 1B C2 D7 89 E6 92 6D 64 3A 2C 35
59 18 B9 39 A9 21 E7 AA F2 BA 2A F8 A2 87 24 1D
29 25 8A 2D C0 6C 6E 4C 3F 58 51 6F 85 56 91 A4
```

Рис. 14. Значення S – блоків S_{41} (зліва) та S_{42}

```
EF 6E D7 68 3D 91 8D E2 6B 10 0E 35 CC 18 63 44
36 45 1E B6 43 7A 00 F3 12 B9 66 CF FF 07 4B 1C
1B 8E FB 9F 05 70 67 C8 5F 50 C9 BC 0B F5 C1 1A
46 65 C0 E5 F1 14 01 9A 0D 5E E4 88 6F AB 41 13
09 53 E9 A4 33 F7 95 79 06 84 A0 58 99 94 49 AE
A6 27 A8 BF E3 BE 4D 4C 57 EA 7C 42 DD 86 FD 87
A2 C4 EE A3 85 C3 64 93 DF 7F B0 76 C7 D3 ED AD
A9 E8 26 3A 38 B2 2C 73 CA 52 F0 31 19 39 4F D8
EC 81 89 74 E7 6C 69 15 CD 5A 8B B4 61 FE 3F DE
A5 E6 30 9B C2 0C F4 D9 08 C5 2E D6 8C FA 04 29
BA 3E 03 BB E0 0F 17 2D 9D 21 A7 D2 6D 82 4E 7D
2F 90 CB 92 D1 59 71 8A 6A A1 DC 34 5D D5 3B 83
98 AF 20 BD 5B AC 25 11 B7 FC EB 48 7E 77 8F D0
3C 40 56 47 72 F8 CE 55 4A F9 2B F2 75 80 60 7B
51 AA 62 D4 97 23 B8 96 2A 54 24 1F E1 9C C6 32
DA B5 37 16 F6 B1 B3 22 1D DB 0A 02 9E 78 5C 28
```

```
9F 95 69 3B 9E D3 99 93 2F E0 63 9B 94 2C 85 C0
56 82 E7 87 F1 8A 5F 00 97 1F 06 84 E5 EE CE 6A
71 F3 29 6B C7 43 F4 15 1C 8E 3D DE 40 01 C8 C9
51 B4 8F 12 20 96 3A F5 1A D9 59 D6 D5 67 C3 44
A2 A3 B9 7E 34 83 F2 5B A4 7B 58 45 92 BB F0 77
0D C2 D4 60 17 50 6C FB 3E 47 DD D2 6F 18 B0 CA
6E 27 54 FD AA 1E 2B BE 07 E2 3F 33 26 4D A0 10
CD 68 4C 37 49 A8 22 E4 39 64 ED 79 42 02 D0 4E
70 7D F8 0E AF C1 25 0C F9 9A AB B7 2E 38 41 B3
2D CF FC 21 4B A7 31 DF F7 52 89 81 13 E6 CB 23
B8 0B 32 A9 7C 72 5A 05 5D 28 0F B5 FE 16 4A 7A
61 BA 24 08 8B 98 AD 36 D7 EA 86 75 DC A1 C6 E1
53 AE B1 AC 74 55 48 EC 9D EF C4 35 19 62 A6 14
76 C5 5C BD 0A FF F6 91 7F 9C 04 11 E9 B2 30 1D
57 2A 66 BF 90 80 E8 FA B6 BC 09 E3 1B 78 73 4F
8C DB 03 6D 88 A5 CC 3C 8D 46 EB D1 D8 65 DA 5E
```

Рис. 15. Значення S – блоків S_{43} (зліва) та S_{44}

Таблиця 5

Параметри s-блоків S_{41} - S_{44} , що задовольняють умові (13)

s-блок	$\Delta^{s}_{+,\oplus}$	$\Delta^{s}_{+,+}$	s-блок	$\Delta^{s}_{+,\oplus}$	$\Delta^{s}_{+,+}$
S_{41}	0,0234375	0,03125	S_{42}	0,046875	0,03125
S_{43}	0,0390625	0,03125	S_{44}	0,0390625	0,03125

Висновки

Отримані результати свідчать про те, що імовірність співпадіння результатів модульного та покомпонентного додавання (віднімання) є дуже малою. Вона зменшується із зростанням довжини вектора (або ключового суматора) і прямує до нуля, коли довжина вектора прямує до нескінченості. Тому використання для аналізу стійкості блокового алгоритму такої його модифікації, в якій модульне додавання (віднімання) замінюється на покомпонентне, є некоректним, хоч і суттєво спрощує аналіз алгоритму.

Крім того, показано, що заміна операції у ключовому суматорі або блоку підстановки шифру недопустима без попередніх досліджень, що полягають в обчисленні і порівнянні відповідних параметрів. Якщо ж є додаткова інформація про те, що відбулись модифікації шифру, вказані у розділі 4, то модифікований шифр може бути більш вразливим до різницевих методів криптоаналізу. Аналогічно, якщо отримано додаткову інформацію про те, що під час дослідження криптографічної стійкості шифру розглядалась лише його відповідна модифікація, то сам шифр може виявитись вразливим до різницевих атак.

Література

[1]. A. Konheim, *Computer security and cryptography,* J.Wiley&Sons, Inc. Hoboken, New Jersey. 2007, 521 p.

[2]. M. Stamp, R. Low, *Applied cryptoanalysis: breaking ciphers in the real world*, J.Wiley&Sons, Inc. Hoboken, New Jersey, 2007, 401 p.

[3]. С. Панасенко, *Алгоритмы шифрования. Специальный справочник,* СПб.: БХВ-Петербург, 2009, 576 с.

[4]. А. Грушо, Э. Применко, Е. Тимонина, *Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений*, М.: Изд.центр Академия, 2009, 272 с.

[5]. Г. Гулак, "Моделирование на этапе оценки безопасности шифраторов конфиденциальной информации", *Науково-практичний журнал «Сучасна спеціальна техніка»,* № 1(24), С. 73-81, 2011.

[6]. Г. Гулак, "Забезпечення безпеки засобів КЗІ у кіберпросторі", *Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології», том ІУ Сучасні технології інформаційної безпеки*, К., С. 100-102, 2015.

[7]. Г. Гулак Г.М. "Оцінка інженерно криптографічних якостей під час тематичних досліджень криптосистем", *13 Міжнародна науково практична конференція «Математичне та імітаційне моделювання систем МОДС 2018» Київ, Чернігів Жукін, 25...29 червня 2018. Тези доповідей*. Чернігів ЧНТУ, С. 326-330, 2018.

[8]. Г. Гулак, П. Складанний, "Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури", *II Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одесса, 17 листопада 2017р.),* Одесса: ОДУВС, С. 12-14, 2017.

[9]. К. Шеннон, "Теория связи в секретных системах", *Работы по теории информации и кибернетике*, М.: Издательство иностранной литературы, С. 333-402, 1963.

[10]. Ю. Горчинский, "О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями", Труды по дискретной математике, Т. 1, М.: ТВП, С. 67– 84, 1997.

[11]. О. Шемякина, "О перемешивающих свойствах операций в конечном поле", *Труды Восьмой Общероссийской научной Конференции «Математика и безопасность информационных технологий» – (МаБИТ-09), 30 октября – 2 ноября 2009.*

[12]. Л. Ковальчук, О. Сиренко, "Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе", *Кибернетика и системный анализ*, № 5, С. 83-97, 2011.

[13]. Л. Ковальчук, О. Сиренко, "Анализ перемешивающих свойств операций в конечном кольце", *Сборник тезисов XIV Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах», 17-20 мая 2011*, Киев, С. 45-46, 2011.

[14]. Л. Ковальчук, Н. Лысенко, Л. Скрыпник, "Перемешивающие свойства операций, определенных на множестве N-мерных векторов над простым конечным полем", *Кибернетика и системный анализ,* № 4, С. 135-145, 2014.

[15]. *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*. М.: Госстандарт СССР, 1989, 28 с.

[16]. И. Горбенко, М. Бондаренко, "Перспективний блоковий шифр «Мухомор» – основні положення та специфікація", *Прикладна радіоелектроніка*, Т. 6. №2, С. 147-157, 2017.

[17]. И. Горбенко, О. Тоцький, С. Казьміна, "Перспективний блоковий шифр «Калина» – основні положення та специфікація", *Прикладна радіоелектроніка*, Т. 6, №2, С. 195-208, 2007.

[18]. В. Галинский, "Вероятностные свойства переносов при сложении по модулю 2^n", *Обозрение прикладной и промышленной математики*, Т. 10, вып. 1, С. 129-130, 2003.

[19]. Л. Ковальчук, С. Пальченко, Л. Скрыпник, "Построение верхних оценок средних вероятностей целочисленных дифференциалов для композиции ключевого сумматора, блока подстановки и оператора циклического сдвига", *Труды Восьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-09), Москва, 30 октября – 2 ноября 2009*, С. 74-87, 2010.

УДК 621.3.019.3+004.056

Гулак Г.Н. Анализ операций модульного и покомпонентного прибавления в блоковых шифрах

Аннотация. *В работе исследуются свойства операций модульного и покомпонентного сложения, которые используются в узлах блочных шифров и обеспечивают сложение ключевой информации (ключевые сумматоры), и их влияние на практическую криптографическую стойкость. Для этого получены вспомогательные*

результаты для функций распределения вероятностей обычных и модульных сумм независимых равномерно распределенных случайных величин. В основной части доказано, что последовательность битов переноса в следующий разряд при модульном сложении чисел образует однородную цепь Маркова с определенным начальным состоянием и соответствующей матрицей переходов, а также выведена формула вероятности того, что при модульном и покомпонентном сложении в результате образуется переходов между блоками, в которых все компоненты совпадают, и блоками, в которых все компоненты не совпадают. С учетом вспомогательных результатов в статье получены и сравнены вероятностные характеристики операций покомпонентного та модульного сложения, вычислены вероятности совпадения результатов этих операций, сделаны выводы о корректности (некорректности) использования соответствующих модификаций блочных шифров для получения оценок стойкости, приведены практически применимые образцы блоков замены для блочных шифров, которые соответствуют определенным условиям, определена возможность уязвимости шифра к определенным типам разностных атак при условии наличия дополнительной информации о том, что при оценке стойкости данного шифра использовалась его модификация, полученная путем замены операции в ключевом сумматоре на некоторую другую. В статье обоснован вывод, что замены операции в ключевом сумматоре или блоков подстановок шифра недопустима без предварительных исследований, суть которых в вычислении и сравнении соответствующих параметров.

Ключевые слова: *блочный шифр, блок замени, ключевой сумматор, операция модульного сложения, операция покомпонентного сложения, криптографическая стойкость.*

Hulak H. Analysis of modular and component addition operations in block codes

Abstract. *The paper investigates the properties of modular and componentwise addition operations, which are used in the nodes of block ciphers and provide the addition of key information (key adders), and their impact on practical cryptographic security. For this, auxiliary results are obtained for the probability distribution functions of ordinary and modular sums of independent uniformly distributed random variables. In the main part, it is proved that the sequence of carry bits in the next bit during modular addition of numbers is a homogeneous Markov chain with a certain initial state and the corresponding transition matrix, and also a formula for the probability that, during modular and componentwise addition, transitions between blocks are formed in which all components match, and blocks in which all components do not match. Taking into account the auxiliary results in the article, the probabilistic characteristics of the operations of componentwise and modular addition are obtained and compared, the probabilities of the coincidence of the results of these operations are calculated, conclusions are drawn about the correctness (incorrectness) of using the corresponding modifications of block ciphers to obtain security estimates, practically applicable samples of replacement blocks for block ciphers are given that correspond to certain conditions, the possibility of vulnerability of the cipher to certain types of differential attacks is determined, provided there is additional information that when assessing the strength of this cipher, its modification was used, obtained by replacing the operation in the key adder with some other. The article substantiates the conclusion that replacing an operation in a key adder or cipher substitution blocks is unacceptable without preliminary research, the essence of which is the calculation and comparison of the corresponding parameters.*

Keywords: *block cipher, substitute block, key adder, modular addition operation, component addition operation, cryptographic strength*

Гулак Геннадій Миколайович, кандидат технічних наук, доцент, завідувач лабораторії досліджень кібербезпеки Інституту проблем математичних машин і систем Національної академії наук України.
Гулак Геннадий Николаевич, кандидат технических наук, доцент, заведующий лаборатории исследований кибербезопасности Института проблем математических машин и систем Национальной академии наук Украины.
Hulak Hennadii, Candidate of Technical Sciences (Information security), Associate Professor, Head of the Cybersecurity Research Laboratory of the Institute for Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine.

Отримано 01 *серпня 2020 року*, затверджено редколегією *14 серпня 2020 року*