Людмила Ковальчук, Наталія Лисенко*, Сергій Красніков*
*ІСЗЗІ НТУУ «КПІ», *ДержНДІ Спецзв'язку*
УДК 621.391:519.2:519.7

ПОРІВНЯННЯ ОПЕРАЦІЙ МОДУЛЬНОГО ТА ПОКОМПОНЕНТНОГО ДОДАВАННЯ І ВІДНІМАННЯ НА МНОЖИНІ N-МІРНИХ ВЕКТОРІВ НАД ПРОСТИМ СКІНЧЕННИМ ПОЛЕМ

Анотація: **Наведені оцінки імовірностей збігу результатів операцій покомпонентного та модульного додавання (віднімання) на множині *n*-мірних векторів над простим скінченним полем.**
Summary: **Above estimates the probability coincidence results the influence of the component-wise/modular addition (subtraction) of N-dimensional vectors over a prime finite field.**
Ключові слова: **Покомпонентне додавання, модульне додавання, ймовірність.**

Вступ

Як відомо, традиційною основою забезпечення конфіденційності інформації в сучасних інформаційних та телекомунікаційних системах є симетричні криптосистеми, серед яких у системах захисту інформації в обчислювальних мережах, автоматизованих системах керування, збереження та обробки даних важливе місце посідають блокові шифри (далі – БШ).

Найважливішою вимогою, що висувається до сучасних БШ, є практична криптографічна стійкість відносно всіх відомих на даний час криптоаналітичних атак.

Варто зазначити, що традиційний підхід до побудови сучасних блокових шифрів ґрунтується на загальноприйнятих принципах – розсіюванні та перемішуванні, сформульованих ще у фундаментальній роботі К. Шеннона [1]. Під розсіюванням мається на увазі вплив одного знаку відкритого тексту на багато знаків шифрованого тексту, що дозволяє «згладити» статистичні властивості відкритих повідомлень. Принципом перемішування К. Шеннон назвав руйнування статистичних залежностей між відкритим та шифрованим текстом при криптографічному перетворенні. Тому найбільш поширеним методом побудови БШ на сьогоднішній день є метод, заснований на застосуванні так званих ітераційних схем, в яких шифруючі перетворення реалізуються у вигляді суперпозиції досить простих перетворень (з точки зору програмної реалізації та обчислювальної складності), кожне з яких вносить невеликий внесок в істотне сумарне розсіювання і перемішування. Таким чином, необхідна криптографічна стійкість даного шифру досягається за рахунок застосування великої кількості простих перетворень, які в сукупності забезпечують «хороші» перемішувальні та розсіювальні властивості. В зв'язку з цим виникає питання про знаходження такого набору операцій на множині бітових векторів (відкритих текстів), які, з одного боку, зручно реалізуються і програмним, і апаратним способом, а з іншого – володіють «хорошими» перемішуючими властивостями [2 – 5, 7].

Дуже часто при оцінюванні стійкості БШ до різних методів криптоаналізу (особливо до лінійного та різницевого криптоаналізу) автори відповідних робіт намагаються замість шифру використовувати його спрощену модифікацію. Так, 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" [8 – 10]. Там операція додавання за модулем 2^{32} замінюється операцією побітового додавання, що суттєво спрощує аналіз цього шифру. Якихось обґрунтованих аргументів стосовно математичної коректності такої заміни у роботах не наводиться; лише деякі міркування відносно того, що при заміні нелінійної (відносно $\boxplus$) операції на лінійну стійкість алгоритму не зростає. Оскільки такі міркування зустрічаються досить часто, то в результаті постає питання: " Чи можна при оцінці криптографічної стійкості алгоритму замінювати одну операцію на іншу, отримувати 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 (віднімання);

- обчислення імовірностей збігу результатів операцій покомпонентного та модульного додавання (віднімання);
- отримання висновків щодо коректності використання відповідних модифікацій БШ для побудови оцінок стійкості самого шифру.

Схожі питання для побітових операцій розглянуті в [10], проте у цій роботі отримано узагальнення її результатів на випадок довільного простого модуля *p*, але лише в окремому випадку двох доданків.

I Допоміжні позначення та результати

При доведенні основних результатів будуть використовуватись наступні позначення та твердження. Тут і надалі під $(V_n(p),\oplus_p)$ будемо розуміти множину векторів довжини n з операцією покомпонентного додавання за модулем простого числа *p*, а під $(Z_{p^n},+)$ – 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 $\{0, \dots, a-1\}$, $a \in N$. 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

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

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

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

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

та

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

то

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

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (28), 2014 р.

і

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

Лему доведено.

Лема 2

Нехай випадкові величини *x* та *y* рівноімовірно розподілені на групі $(Z_{p^n}, +)$. Тоді

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

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 $P(x \leq y) = 1 - P(x > y)$; 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

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

а

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

В наших позначеннях, $P(x > y) = \frac{1}{2} - \frac{1}{2p^n} = q_n$ та $P(x \leq y) = \frac{1}{2} + \frac{1}{2p^n} = s_n$.

Лему доведено.

II 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:

$$v_0 = 0,$$

$$v_i = \begin{cases} 0, \text{ якщо } a_{i-1} + b_{i-1} + v_{i-1} < p \\ 1, \text{ інакше.} \end{cases}, \partial e\ i = 1, ..., n-1.$$

Зрозуміло, що v_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 на $Z_p{}^n$. Тоді:

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

Доведення: з означення v_i, випливає, що

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

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 $\nu_i, i \geq 1,$ 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,

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

Тому

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

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

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

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

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

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

Теорему доведено.

Сформуємо 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 7.1, $P(y_i = z_i) = P(\nu_i = 0) = \frac{1}{2} + \frac{1}{2p^i}$. Наслідок доведено.

Наслідок 6: за наших позначень $P(y = z) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}$.

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

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

Наслідок доведено.

Наслідок 7: за наших позначень 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 $k = 1, ..., n\text{-}1$.

Доведення:

$$P(y_0 = z_0, y_1 = z_1, ..., y_{k-1} = z_{k-1}, y_k \neq z_k, y_{k+1} \neq z_{k+1}, ..., y_{n-1} \neq z_{n-1},) = P(\nu_0 = 0) \cdot P(\nu_1 = 0 / \nu_0 = 0) \times$$

$$\times P(\nu_2 = 0 / \nu_1 = 0) \cdot ... \cdot P(\nu_{k-1} = 0 / \nu_{k-2} = 0) \cdot P(\nu_k = 1 / \nu_{k-1} = 0) \cdot P(\nu_{k+1} = 1 / \nu_k = 1) \cdot P(\nu_{k+2} = 1 / \nu_{k+1} = 1) \cdot ... \times$$

$$\times P(\nu_{n-1} = 1 / \nu_{n-2} = 1) = 1 \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right) \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right).$$

Наслідок 8: імовірність того, що при модульному та покомпонентному додаванні в результаті утвориться $k < n\text{-}1$ переходів між блоками, в яких всі компоненти збігаються, та блоками, в яких всі компоненти не збігаються, 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 наслідка 7.

III Порівняння 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 параграфу 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

$$P(\mu_i = {}^{a}\!/_{\mu_{i-1},\ldots,\mu_0}) = P(\mu_i = {}^{a}\!/_{\mu_{i-1}}),$$

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

$$P_{11} = P(\mu_i = {}^{1}\!/_{\mu_{i-1}} = 1) = P(a_{i-1} - 1 < b_{i-1}) = P(a_{i-1} < b_{i-1} + 1) = \sum_{k=0}^{p-1} P\left(a_{i-1} < b_{i-1} + 1 \,/\, a_{i-1} = \kappa\right) \times$$

$$\times P(a_{i-1} = \kappa) = \sum_{k=0}^{p-1} P\left(k < b_{i-1} + 1\right) \cdot P(a_{i-1} = \kappa) = \frac{1}{p} \cdot (p + p - 1 + p - 2 + \ldots + 1) \cdot \frac{1}{p} = \frac{1}{p} \cdot \frac{1+p}{2} \cdot p \times$$

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

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

$$P_{10} = P(\mu_i = {}^{0}\!/_{\mu_{i-1}} = 1) = P(a_{i-1} - 1 \geq b_{i-1}) = 1 - P(a_{i-1} - 1 < b_{i-1}) = 1 - (\frac{1}{2} + \frac{1}{2p}) = \frac{1}{2} - \frac{1}{2p} = q_1;$$

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

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

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

$$P(w = u) = P(\bigcap_{i=0}^{n-1} \{w_i = u_i\}) = P({}^{w_{n-1} = u_{n-1}}\!/_{w_0 = u_0, \ldots, w_{n-2} = u_{n-2}}) \times$$

$$P({}^{w_{n-2} = u_{n-2}}\!/_{w_0 = u_0, \ldots, w_{n-3} = u_{n-3}}) \cdot \ldots \cdot P({}^{w_1 = u_1}\!/_{w_0 = u_0}) = P({}^{\mu_{n-1} = 0}\!/_{\mu_0 = 0, \ldots, \mu_{n-2} = 0}) \times$$

$$\times P({}^{\mu_{n-2} = 0}\!/_{\mu_0 = 0, \ldots, \mu_{n-3} = 0}) \cdot \ldots \cdot P({}^{\mu_1 = 0}\!/_{\mu_0 = 0}) \cdot P(\mu_0 = 0) = P({}^{\mu_{n-1} = 0}\!/_{\mu_{n-2} = 0}) \cdot$$

$$P({}^{\mu_{n-2} = 0}\!/_{\mu_{n-3} = 0}) \cdot \ldots \cdot P({}^{\mu_1 = 0}\!/_{\mu_0 = 0}) \cdot 1 = s_1^{n-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Наслідок доведено.

Наслідок 13: за наших позначень виконується рівність

$$P(w_0 = u_0, w_1 = u_1, ..., w_{k-1} = u_{k-1}, w_k \neq u_k, w_{k+1} \neq u_{k+1}, ..., w_{n-1} \neq u_{n-1},) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right),$$

де $k = 1, ..., n-1$.

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 збігаються, та блоками, в яких всі компоненти не збігаються, 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.

Висновки

Отримані результати свідчать про те, що імовірність збігу результатів модульного та покомпонентного додавання (віднімання) є дуже малою. Вона зменшується зі 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.

Список використаної літератури: ***1.*** *Шеннон К. Теория связи в секретных системах //Работы по теории информации и кибернетике. – М.: Издательство иностранной литературы, 1963. – С. 333-402.* ***2.*** *Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр всвязи с криптографическими применениями // Труды по дискретной математике. Т. 1. – М.: ТВП, 1997. – с. 67– 84.* ***3.*** *О. В. 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.* ***4.*** *Л. В. Ковальчук, О. А. Сиренко. Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе. // Кибернетика и системный анализ. – 2011. – № 5. – с. 83 – 97.* ***5.*** *Л. В. Ковальчук, О. А. 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.* ***6.*** *Ковальчук Л. В., Лысенко Н. В., Скрыпник Л. В. Перемешивающие свойства операций, определенных на множестве N-мерных векторов над простым конечным полем // Кибернетика и системный анализ. – 2014. – № 4. – С.135 – 145.* ***7.*** *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989. – 28 стр.* ***8.*** *Горбенко И. Д., Бондаренко М.Ф. та ін. Перспективний блоковий шифр "Мухомор" – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. – т.6. №2. – с. 147 – 157.* ***9.*** *Горбенко И. Д., Тоцький О. С., Казьміна С. В. Перспективний блоковий шифр «Калина» – основні положення та специфікація // Прикладна радіоелектроніка. – 2007. - т. 6, № 2. –.с.195 – 208.* ***10.*** *Галинский В. А. Вероятностные свойства переносов при сложении по модулю 2^n // Обозрение прикладной и промышленной математики. 2003. Т. 10, вып. 1. с. 129 – 130.*