CRYPTOLOGY

DOI 10.20535/2411-1031.2025.13.1.328762
УДК 004.056

АЛЕКСАНДРА МАТІЙКО,
АНТОН ОЛЕКСІЙЧУК

СТАТИСТИЧНА АТАКА НА КОМБІНУВАЛЬНІ ГЕНЕРАТОРИ ГАМИ З НЕРІВНОМІРНИМ РУХОМ

Комбінувальні генератори гами з нерівномірним рухом є основою для побудови низки потокових шифрів, найвідомішими з яких є шифри сім'ї *A*5 та Alpha1. Кожен такий генератор складається з декількох двійкових лінійних регістрів зсуву, булевої комбінувальної функції та блоку управління рухом регістрів, який визначає правила, за якими останні зсуваються в процесі вироблення шифрувальної гами. Незважаючи на певні слабкості відомих потокових шифрів, побудованих на базі комбінувальних генераторів гами з нерівномірним рухом, такі генератори досі викликають теоретичний та прикладний інтерес внаслідок простоти їхньої будови та потенційної здатності забезпечувати стійкість до широкого класу атак за умови належного вибору їхніх компонент.

У статті досліджуються комбінувальні генератори гами, кожен регістр яких або зсувається на один крок, або простоює в кожному такті, причому один з регістрів рухається рівномірно. Раніше авторами статті показано, що зазначеним генераторам притаманна слабкість, яка полягає у статистичній залежності між кожними сусідніми знаками їхніх вихідних послідовностей. Основним результатом цієї статті є статистична атака, яка базується на зазначеній слабкості. Запропонована атака спрямована на відновлення початкового стану регістру, що рухається рівномірно, за відомою вихідною послідовністю генератора або декількома такими послідовностями, які виробляються генератором в режимі реініціалізації початкового стану. Показано, що в останньому випадку складність атаки залежить лінійно від довжини зазначеного регістру. Отримано аналітичну оцінку обсягу матеріалу, потрібного для реалізації запропонованої атаки з потрібною достовірністю. Зокрема, показано, що для шифру Alpha1 відповідний обсяг матеріалу становить приблизно 300 відрізків гами поряд з відповідними їм векторами ініціалізації. Сформульовано умови, які послаблюють стійкість генераторів з нерівномірним рухом відносно запропонованої атаки. Вони полягають в тому, що коефіцієнти Уолша-Адамара комбінувальної функції приймають нульові значення на всіх векторах ваги 0 і 1 та ненульові значення на певних векторах ваги 2. Показано, що ці умови виконуються для генератора гами шифру Alpha1. При цьому середній обсяг матеріалу, потрібного для відновлення початкового стану довільного генератора гами, який задовольняє наведені умови, є за порядком таким самим, що і для шифру Alpha1.

Ключові слова: криптографічний захист інформації, комбінувальний генератор гами з нерівномірним рухом, статистична атака, перетворення Уолша-Адамара, *A*5/1, Alpha1.

Постановка проблеми. Комбінувальні генератори гами (КГГ) з нерівномірним рухом лінійних регістрів зсуву (ЛРЗ) є класичним об'єктом дослідження у криптографії. Найвідомішими прикладами таких КГГ є генератори гами потокових шифрів *A*5/1 [1] та Alpha1 [2], запропонованих понад 25 років тому. Незважаючи на відомі слабкості в конструкціях цих шифрів та наявність великої кількості атак на них [1], [3]–[8], КГГ з нерівномірним рухом досі викликають теоретичний та прикладний інтерес внаслідок простоти їхньої будови та потенційної здатності забезпечувати стійкість до широкого класу атак за умови належного вибору їхніх компонент (див., наприклад, нещодавню роботу [9], присвячену побудові нових атак на шифр *A*5/1).

З практичних міркувань викликають інтерес такі КГГ, кожен регістр яких або зсувається на один крок, або простоює в кожному такті (зауважимо, що генератори гами шифрів $A5/1$ та Alpha1 задовольняють цю вимогу). В роботі [10] показано, що зазначеним КГГ притаманна певна слабкість, яка полягає у статистичній залежності між кожними сусідніми знаками вихідних послідовностей таких генераторів гами. Виникає природне запитання, чи може ця потенційна слабкість призводити до реальних атак на зазначені КГГ з нерівномірним рухом.

Мета статті полягає в тому, щоб надати (позитивну) обґрунтовану відповідь на це запитання.

Аналіз останніх досліджень і публікацій. Традиційна ймовірнісна модель КГГ з нерівномірним рухом визначається таким чином [3], [11]–[14]. Генератор гами складається з n ЛРЗ з примітивними многочленами зворотного зв'язку, зрівноваженої комбінувальної функції $f = f(z_1, \dots, z_n)$ та блоку управління рухом ЛРЗ, який виробляє послідовності невід'ємних цілочисельних векторів $\varepsilon(i) = (\varepsilon_1(i), \dots, \varepsilon_n(i))$, $i = 0, 1, \dots$, де для будь-яких $j \in \overline{1, n}$, $i = 0, 1, \dots$. число $\varepsilon_j(i)$ дорівнює величині зсуву j-го ЛРЗ у i-му такті.

Якщо $X_j(0), X_j(1), \dots$ – лінійна рекурентна послідовність, яка виробляється за початковим станом j-го ЛРЗ у режимі рівномірного руху, $j \in \overline{1, n}$, то знак вихідної послідовності КГГ в i-му такті визначається за формулою

$$\gamma_i = f(X_1(\delta_1(i)), \dots, X_n(\delta_n(i))), \ i = 0, 1, \dots,$$

де

$$\delta_j(0) = 0, \ \delta_j(i) = \sum_{k=0}^{i-1} \varepsilon_j(k), \ i = 1, 2, \dots, \ j \in \overline{1, n}.$$

Надалі вважатимемо, що $\varepsilon(i)$, $i = 0, 1, \dots$, є незалежними однаково розподіленими двійковими випадковими векторами, а $X_j(0), X_j(1), \dots$ є випадковою рівноймовірною послідовністю, що не залежить від векторів $\varepsilon(i)$, $i = 0, 1, \dots$.

Найвідомішими прикладами зазначених КГГ є генератори гами шифрів $A5/1$ [1] та Alpha1 [2]. Останній складається з $n = 4$ ЛРЗ R_1, R_2, R_3, R_4 довжини 29, 31, 33, 35 відповідно та комбінувальної функції $f = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_2 z_3$. При цьому регістр R_1 рухається рівномірно, а закон руху решти ЛРЗ описується у ймовірнісних термінах згідно з табл. 1 у [10].

Одну з найперших статистичних атак на КГГ з нерівномірним рухом запропоновано в [3] для шифру $A5/1$. Згодом метод побудови таких атак розвинено та узагальнено в [11]–[14] на довільні КГГ з нерівномірним рухом. У [8] досліджено кореляційні властивості вихідних послідовностей генератора гами шифру Alpha1, які використано в [15, 16] для побудови ефективних атак на нього. В [10] встановлено явний вираз ймовірності збігу двох сусідніх знаків вихідної послідовності довільного КГГ, побудованого на базі ЛРЗ, кожен з яких або простоює або зсувається на один крок в кожному такті. Зокрема, в [10] (див. наслідки 1 та 2) отримано такий результат.

Твердження 1. Нехай ЛРЗ R_1 рухається рівномірно, а функція f має порядок кореляційної імунності не менше 1. Тоді для будь-якого $i = 0, 1, \dots$ ймовірність події

$$\{X_1(i) \oplus X_1(i+1) \oplus f(X(\delta(i))) \oplus f(X(\delta(i+1))) = 0\}$$

визначається за формулою

$$\tilde{\pi}_f = \frac{1}{2}\left(1 + 2^{-2n} \sum_{\beta \in V_{n-1} \setminus \{0\}} |W_f((1, \beta))|^2 p_\varepsilon((1, \beta))\right), \qquad (1)$$

де

$$W_f(\alpha) = \sum_{x \in V_n} (-1)^{f(x) \oplus \alpha x}$$

є перетворенням Уолша-Адамара функції f,

$$p_\varepsilon(\alpha) = \Pr\{\varepsilon_{i_1}(i) = 0, ..., \varepsilon_{i_s}(i) = 0\},$$

$\{i_1, ..., i_s\} = \mathrm{supp}(\alpha)$ – носій (множина номерів ненульових координат) довільного вектора $\alpha \in V_n \setminus \{0\}$, $i = 0, 1, ...$. Зокрема, для генератора гами шифру Alpha1 ймовірність (1) (збігу будь-яких сусідніх знаків випадкової послідовності, яка отримується шляхом додавання виходу регістру R_1 до вихідної послідовності генератора) становить $0{,}625$.

Виклад основного матеріалу дослідження. В [8] запропоновано статистичну атаку на шифр Alpha1, яка спрямована на відновлення початкового стану ЛРЗ R_1 за відрізком $\gamma_0, \gamma_1, ..., \gamma_t$ вихідної послідовності генератора. Зазначена атака базується на відмінності ймовірності (1) від $1/2$ та аналогічна по суті відомій атаці Зігенталера (див., наприклад, [17]).

Переберемо всі $2^{29} - 1$ ненульових початкових станів ЛРЗ R_1, для кожного з яких обчислимо перші t знаків послідовності

$$z(i) = x_1(i) \oplus x_1(i+1) \oplus \gamma_i \oplus \gamma_{i+1},\ i = 0, 1, ..., \qquad (2)$$

де $x_1(0), x_1(1), ...$ – лінійна рекурента, яка виробляється ЛРЗ R_1 за початковим станом $x_1 \in V_{29}$ (тут і далі V_n позначає множину двійкових векторів довжини n).

Припустимо, що послідовність (2) є реалізацією схеми Бернуллі з ймовірністю успіху (появи нуля) p_{x_1}. Тоді, згідно з твердженням 1, для справжнього значення x_1 маємо $p_{x_1} = \tilde{\pi}_f = 0{,}625$, в той час як для хибних значень x_1 виконується рівність $p_{x_1} = 0{,}5$. Отже, застосовуючи відомі статистичні критерії, можна розрізнити два зазначені випадки з як завгодно високою достовірністю за наявності достатнього обсягу матеріалу. Для оцінки останнього можна скористатися наближеною формулою: $t_f = C(\tilde{\pi}_f - 0{,}5)^{-2} = 2^6 C$, де значення C залежить лише від ймовірностей помилок першого і другого роду статистичного критерію, що використовується (див., наприклад, [17]).

Зауважимо, що незначна, на перший погляд, модифікація в конструкції генератора гами шифру Alpha1 приводить до суттєвого збільшення значення t_f, а отже, й до підвищення стійкості цього шифру відносно статистичної атаки, що розглядається. Дійсно, розглянемо функцію $f' = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_1 z_4$, яка відрізняється від комбінувальної функції $f = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_2 z_3$ лише перестановкою змінних. Застосовуючи до f' твердження 1 та використовуючи дані табл. 1 у [10], отримаємо таке значення ймовірності (1):

$$\tilde{\pi}_{f'} = 1/2 \cdot \left(1 + 2^{-2}(\Pr\{\varepsilon_2(0) = \varepsilon_3(0) = 0\} + \Pr\{\varepsilon_2(0) = \varepsilon_3(0) = \varepsilon_4(0) = 0\})\right) = 1/2 \cdot (1 + 2^{-5}).$$

Отже, для успішного проведення статистичної атаки на модифікацію шифру Alpha1, яка отримується шляхом заміни функції f на функцію f', потрібно (при тих самих ймовірностях помилок першого та другого роду) приблизно $t_{f'} = C(\tilde{\pi}_{f'} - 0{,}5)^{-2} = 2^{12} C$ знаків гами, тобто в 64 рази більше у порівнянні зі значенням t_f.

Покажемо, що описану статистичну атаку можна, в принципі, здійснити на будь-який КГГ з нерівномірним рухом, який задовольняє умову твердження 1. При цьому не обов'язково перебирати усі початкові стани ЛРЗ R_1.

Дійсно, нехай $X_1(0), X_1(1), \ldots$ – невідома вихідна послідовність ЛРЗ R_1, $\gamma_i = f(X_1(i), X_2(\delta_2(i)), \ldots, X_n(\delta_n(i)))$ – знак гами, що виробляється генератором в i-му такті. Позначимо $X(i) = (X_1(i), X_2(\delta_2(i)), \ldots, X_n(\delta_n(i)))$, $\tilde{X}_1(i) = X_1(i) \oplus X_1(i+1)$, $\tilde{\gamma}_i = \gamma_{i+1} \oplus \gamma_i$, $\xi_i = g(X(i)) \oplus g(X(i+1))$, $i = 0, 1, \ldots$, де $g(z_1, \ldots, z_n) = z_1 \oplus f(z_1, \ldots, z_n)$, $(z_1, \ldots, z_n) \in V_n$. Тоді знаки лінійної рекуренти $\tilde{X}_1(0), \tilde{X}_1(1), \ldots$ задовольняють систему рівнянь (СР) вигляду

$$\tilde{X}_1(i) \oplus \xi_i = \tilde{\gamma}_i, \ i = 0, 1, \ldots \tag{3}$$

де на підставі твердження 1

$$\Pr\{\xi_i = 0\} = \frac{1}{2}\left(1 + 2^{-2n} \sum_{\beta \in V_{n-1} \setminus \{0\}} |W_f((1, \beta))|^2 p_\varepsilon((1, \beta))\right) > \frac{1}{2}.$$

Для розв'язання СР (3) можна застосувати відомі методи, більш ефективні за трудомісткістю у порівнянні з повним перебором усіх початкових станів ЛРЗ R_1 [17].

Розглянемо зараз окремий випадок, в якому функціонування КГГ з нерівномірним рухом здійснюється в режимі реініціалізації початкового стану (ПС). При цьому, як і досі, вважатимемо, що для даного генератора гами виконується умова твердження 1.

Нагадаємо [11]–[14], що функціонування КГГ в режимі реініціалізації описується системою рівнянь

$$f(X_1^{(l)}(i), X_2^{(l)}(\delta_2^{(l)}(i)), \ldots, X_n^{(l)}(\delta_n^{(l)}(i))) = \gamma_i^{(l)}, \tag{4}$$

$$X_j^{(l)}(i) = X_j^{(0)}(i) \oplus C_j^{(l)}(i), \ i = 0, 1, \ldots, \ j \in \overline{1, n}, \ l \in \overline{1, t}, \tag{5}$$

де $X^{(0)} = (X_1^{(0)}, \ldots, X_n^{(0)})$ – невідомий ПС генератора;

$C^{(1)}, \ldots, C^{(t)}$ – послідовність відомих векторів ініціалізації,

$$C^{(l)} = (C_1^{(l)}, \ldots, C_n^{(l)}), \ C_j^{(l)} = (C_j^{(l)}(0), \ldots, C_j^{(l)}(m_j - 1)) \in V_{m_j}, \ j \in \overline{1, n}, \ l \in \overline{1, t};$$

$C_j^{(l)}(0), C_j^{(l)}(1), \ldots$ – знаки лінійної рекуренти, яка виробляються j-м ЛРЗ генератора (довжини m_j) при рівномірному русі за початковим станом $C_j^{(l)}$;

$\delta^{(l)}(i) = (\delta_1^{(l)}(i), \ldots, \delta_n^{(l)}(i))$ – невідомі вектори, які визначаються згідно із законом функціонування блоку управління рухом КГГ та мають той самий сенс, що й вектори $(\delta_1(i), \ldots, \delta_n(i))$, визначені вище, $i = 0, 1, \ldots$, $j \in \overline{2, n}$, $l \in \overline{1, t}$.

Для відновлення початкового стану ЛРЗ R_1 за відомими векторами $C^{(1)}, \ldots, C^{(t)}$ та знаками гами вигляду (4) складемо та розв'яжемо систему рівнянь, аналогічну СР (3).

Позначимо

$$X^{(l)}(i) = (X_1^{(l)}(i), X_2^{(l)}(\delta_2^{(l)}(i)), \ldots, X_n^{(l)}(\delta_n^{(l)}(i))), \ \tilde{X}_1^{(0)}(i) = X_1^{(0)}(i) \oplus X_1^{(0)}(i+1),$$

$$\tilde{\gamma}_i^{(l)} = \gamma_{i+1}^{(l)} \oplus \gamma_i^{(l)}, \ \xi_i^{(l)} = g(X^{(l)}(i)) \oplus g(X^{(l)}(i+1)), \ i = 0, 1, \ldots, \ l \in \overline{1, t},$$

де $g(z_1, \ldots, z_n) = z_1 \oplus f(z_1, \ldots, z_n)$, $(z_1, \ldots, z_n) \in V_n$.

Припустимо, що члени послідовностей (5) є незалежними рівноймовірними випадковими величинами, що не залежать від випадкових векторів $\delta^{(l)}(i)$, $i = 0, 1, \ldots$, $l \in \overline{1, t}$. Тоді знаки лінійної рекуренти $\tilde{X}_1^{(0)}(0), \tilde{X}_1^{(0)}(1), \ldots$ задовольняють систему рівнянь

$$\tilde{X}_1^{(0)}(i) \oplus \xi_i^{(l)} = \tilde{\gamma}_i^{(l)} \oplus C_1^{(l)}(i) \oplus C_1^{(l)}(i+1), \ i = 0, 1, \ldots, \ l \in \overline{1, t}, \tag{6}$$

де випадкові величини $\xi_i^{(l)}$ мають тій самий закон розподілу, що й ξ_i.

Зауважимо, що СР (6) містить t різних рівнянь відносно кожної невідомої $\tilde{X}_1^{(0)}(i)$, $i = 0, 1, \ldots$, в той час як СР (5) – лише одне таке рівняння. Отже, при $t = O((\tilde{\pi}_f - 0{,}5)^{-2})$, де $\tilde{\pi}_f$ визначається за формулою (1), відновити початковий стан ЛРЗ R_1 можна з лінійною (від його довжини) складністю.

Відновлення початкових станів решти ЛРЗ генератора гами може бути проведено з використанням методу, викладеного в [11 – 14]. Нагадаємо, що його сутність полягає у формуванні та подальшому розв'язанні певної системи лінійних рівнянь (СЛР) зі спотвореними правими частинами відносно елементів початкового стану КГГ.

Вхідними даними для застосування методу є розподіли ймовірностей випадкових векторів $\delta^{(l)}(i)$ ($i = 0, 1, \ldots$, $l \in \overline{1, t}$), вектори ініціалізації $C_j^{(l)}$ ($j \in \overline{1, n}$, $l \in \overline{1, t}$) та відрізки гами вигляду (5), які відповідають зазначеним векторам. Вважається також, що початковий стан ЛРЗ R_1 вже відновлено за допомогою процедури, наведеної вище.

Алгоритм відновлення початкових станів ЛРЗ R_j, $j \in \overline{2, n}$, складається з двох етапів:

1) формування СЛР зі спотвореними правими частинами відносно невідомих $X_j^{(0)}(i)$, $j \in \overline{2, n}$, $i = 0, 1, \ldots$;

2) розв'язання цієї СЛР.

На першому етапі формується множина наборів

$$(a, i_0, \alpha), \tag{7}$$

де i_0 позначає номер знака гами, доступного для аналізу;

$a = (a_1, \ldots, a_n)$ – невід'ємний цілочисельний вектор з властивістю $\Pr\{\delta^{(l)}(i_0) = a\} > 0$;

$\alpha = (\alpha_1, \ldots, \alpha_n)$ – булев вектор такий, що $W_f(\alpha) \neq 0$.

Наведені набори впорядковуються за незростанням значень

$$|\theta(a, i_0, \alpha)| = 2^{-n} |W_f(\alpha)| \pi_{\delta, i0}(a; \alpha), \tag{8}$$

де $\pi_{\delta, i0}(a; \alpha) = \Pr\{\delta_{i_1}(i_0) = a_{i_1}, \ldots, \delta_{i_s}(i_0) = a_{i_s}\}$, $\{i_1, \ldots, i_s\} = \mathrm{supp}(\alpha)$.

Кожному набору (7) ставиться у відповідність лінійна функція

$$\alpha X^{(0)}(a) = \alpha_1 X_1^{(0)}(a_1) \oplus \ldots \oplus \alpha_n X_n^{(0)}(a_n) \tag{9}$$

змінних $X_1^{(0)}(a_1), \ldots, X_n^{(0)}(a_n)$, яка є лівою частиною одного рівняння системи, яку потрібно сформувати. Далі для кожного такого набору з використанням критерію Вальда знаходиться статистична оцінка $\nu = \nu(a, i_0, \alpha)$ значення (9), в результаті чого формуються рівняння вигляду

$$\alpha X^{(0)}(a) = \nu, \tag{10}$$

які утворюють шукану СЛР зі спотвореними правими частинами. Розв'язання отриманої СЛР на другому етапі алгоритму здійснюється стандартним шляхом з використанням відомих методів [17].

Основним параметром, що визначає практичну застосовність викладеного методу, є кількість відрізків гами вигляду (4), доступних для аналізу. Відомо [11], що для відновлення значення (9) з імовірністю не менше $1 - c$, де $c \in (0,\ 1/2)$, достатньо в середньому

$$t(c) = \frac{(1 - 2c) \ln\left(\dfrac{1 - c}{c}\right)}{\theta(a, i_0, \alpha) \ln\left(\dfrac{1 + \theta(a, i_0, \alpha)}{1 - \theta(a, i_0, \alpha)}\right)} \tag{11}$$

знаків послідовності $\gamma_{i_0}^{(1)}, \gamma_{i_0}^{(2)}, \ldots$, причому значення (11) монотонно зростають зі зменшенням параметра $|\theta(a, i_0, \alpha)|$, що визначається за формулою (8). Отже, значення саме цього параметра задають верхню межу ймовірностей спотворень у правих частинах рівнянь (10), від якої, в свою чергу, безпосередньо залежать достовірність ь та складність алгоритмів розв'язання отриманої системи рівнянь.

Припустимо зараз, що порядок кореляційної імунності функції f (див. твердження 1) точно дорівнює 1. Тоді існує булев вектор $\alpha = (\alpha_1, ..., \alpha_n)$ ваги 2 такий, що $W_f(\alpha) \neq 0$. Якщо $\alpha_1 = \alpha_j = 1$, $1 < j \le n$, то на підставі формули (8) отримаємо, що

$$|\theta(a, i_0, \alpha)| = 2^{-n} |W_f(\alpha)| \Pr\{\delta_j(i_0) = a_j\}. \quad (12)$$

Якщо ж $\alpha_{j_1} = \alpha_{j_2} = 1$, де $2 \le j_1 < j_2 \le n$, то, згідно з тою ж формулою

$$|\theta(a, i_0, \alpha)| = 2^{-n} |W_f(\alpha)| \Pr\{\delta_{j_1}(i_0) = a_{j_1}, \delta_{j_2}(i_0) = a_{j_2}\}. \quad (13)$$

Отже, застосовуючи для формування рівнянь (10) всі вектори α ваги 2, яким відповідають ненульові значення $W_f(\alpha)$, отримаємо СЛР зі спотвореними правими частинами такого вигляду:

$$X_1(i_0) \oplus X_j(a_j) = \nu,$$

де $1 < j \le n$;

$$X_{j_1}(a_{j_1}) \oplus X_{j_2}(a_{j_2}) = \nu',$$

де $2 \le j_1 < j_2 \le n$.

Нарешті, використовуючи відомі значення $X_1(0), X_1(1), \ldots$, відновимо початкові стани ЛРЗ R_j та R_{j_1}, R_{j_2}, послідовно розв'язуючи зазначені системи рівнянь. Необхідний для цього обсяг матеріалу можна оцінити заздалегідь за формулами (11)–(13).

Як приклад, що ілюструє наведені загальні міркування, опишемо процедуру відновлення ПС генератора гами шифру Alpha1. Нехай відомо t відрізків

$$\gamma_{i_1}^{(l)}, \ldots, \gamma_{i_2}^{(l)}, \; l \in \overline{1, t}, \quad (14)$$

вихідних послідовностей генератора, які отримані за відомими векторами ініціалізації $C^{(1)}, \ldots, C^{(t)}$ у відповідності з рівностями (4), (5), де для певності $i_1 = 30$, $i_2 = 170$.

Для відновлення початкового стану ЛРЗ R_1 складемо СР вигляду (6) відносно невідомих $\tilde{X}_1^{(0)}(i) = X_1^{(0)}(i) \oplus X_1^{(0)}(i+1)$, $i \in \overline{i_1, i_2 - 1}$. Оскільки така СР містить інформацію про t спотворених значень кожної окремої невідомої, де ймовірність неспотворення $\tilde{\pi}_f = 0{,}625$, то відновити значення усіх невідомих можна зі складністю $O(t(i_2 - i_1))$, використовуючи $t = C(\tilde{\pi}_f - 0{,}5)^{-2} = 64C$ відрізків гами. Значення C залежить від ймовірностей помилок першого і другого роду, що припускаються при відновленні кожної окремої невідомої, та при ймовірностях, не більше за 10^{-2}, не перевищує 5,5. Таким чином, використовуючи приблизно $t = 320$ відрізків гами (19), отримаємо $i_2 - i_1 = 140$ послідовних знаків спотвореної лінійної рекуренти $X_1^{(0)}(0), X_1^{(0)}(1), \ldots$, де ймовірність спотворення кожного знака є не більше за 0,1. Нарешті, використовуючи перевірочні співвідношення для знаків цієї рекуренти, що визначаються многочленом зворотного зв'язку ЛРЗ R_1, відновимо шуканий початковий стан даного регістру зсуву.

Для відновлення ПС решти ЛРЗ складемо лінійні рівняння вигляду

$$X_1(i_0) \oplus X_4(a_4) = \nu, \quad (15)$$

$$X_1(i_0') \oplus X_2(a_2) \oplus X_4(a_4') = \nu',\ X_1(i_0'') \oplus X_3(a_3) \oplus X_4(a_4'') = \nu'' \quad (16)$$

зі спотвореними значеннями ν, ν', ν'' у правих частинах, які відповідають векторам $\alpha = (1, 0, 0, 1)$, $\alpha' = (1, 1, 0, 1)$, $\alpha'' = (1, 0, 1, 1)$ ваги 2 або 3 з властивістю $W_f(\alpha) \neq 0$, $W_f(\alpha') \neq 0$, $W_f(\alpha'') \neq 0$, де f – комбінувальна функція даного генератора гами.

Для побудови рівнянь вигляду (20) обчислимо значення $|\theta(a, i_0, \alpha)|$ за формулою (12) при $j = 4$, $i_0 \in \overline{30, 130}$, $a_4 \in \overline{0, i_0}$. Для цього скористаємося даними табл. 1 в [10], а також тим фактом, що випадкова величина $\delta_4(i_0)$ має біноміальний розподіл ймовірностей з параметрами $(i_0, 9/16)$, звідки на підставі рівності $W_f(\alpha) = 8$ випливає, що

$$|\theta(a, i_0, \alpha)| = \frac{1}{2}\binom{i_0}{a_4}\left(\frac{9}{16}\right)^{a_4}\left(\frac{7}{16}\right)^{i_0 - a_4},\ a_4 \in \overline{0, i_0} \quad (17)$$

Для кожного $a_4 \in \overline{10, 60}$ відберемо дев'ять значень $i_0 \in \overline{30, 130}$, яким відповідають найбільші значення параметра (22), та складемо систему рівнянь (20), використовуючи для оцінювання значень $X_1(i_0) \oplus X_4(a_4)$ критерій Вальда з імовірністю помилки $c = 0{,}1$. Підставляючи в ці рівняння відомі значення $X_1(i_0)$, отримаємо для кожного $a_4 \in \overline{10, 60}$ дев'ять спотворених значень $X_4(a_4)$, де ймовірність спотворення є не більше за $0{,}1$. Нарешті, відновлюючи лінійну рекуренту $X_4(0), X_4(1), \ldots$ за відрізком її слабоспотворених знаків з номерами $a_4 \in \overline{10, 60}$, знайдемо початковий стан ЛРЗ R_4. Середній обсяг потрібного для цього матеріалу визначається за формулою (11) і не перевищує 689 відрізків гами вигляду (19) поряд з відповідними їм векторами ініціалізації (див. табл. 1).

Таблиця 1 – Оцінки середнього обсягу матеріалу, потрібного для відновлення початкового стану ЛРЗ R_4 шифру Alpha1 (при $c = 0{,}1$)

a_4	i_0	$\theta(a, i_0, \alpha)$	$t(c)$
10	14	0,058149	269,63
	15	0,076320	150,60
	16	0,089040	110,56
	17	0,094605	97,90
	18	0,093127	101,05
	19	0,086013	118,51
	20	0,075262	154,87
	21	0,062861	222,14
	22	0,050419	345,45
60	102	0,034872	722,49
	103	0,036544	657,82
	104	0,037790	615,13
	105	0,038577	590,28
	106	0,038892	580,77
	107	0,038737	585,39
	108	0,038131	604,22
	109	0,037110	637,90
	110	0,035718	688,62

Процедура відновлення початкових станів ЛРЗ R_2 та R_3 здійснюється аналогічно на основі формування та розв'язання СР (2).

Висновки. У статті представлено статистичну атаку на комбінувальні генератори гами з нерівномірним рухом, кожен регістр яких або зсувається на один крок, або простоює в кожному такті, причому один з регістрів рухається рівномірно. Запропонована атака спрямована на відновлення початкового стану цього регістру за відомою вихідною послідовністю генератора або декількома такими послідовностями, які виробляються генератором в режимі реініціалізації ПС. Показано, що в останньому випадку складність атаки залежить лінійно від довжини зазначеного регістру. Отримано аналітичну оцінку обсягу матеріалу, потрібного для реалізації запропонованої атаки з потрібною достовірністю. Зокрема, показано, що для шифру Alpha1 відповідний обсяг матеріалу становить приблизно 300 відрізків гами поряд з відповідними їм векторами ініціалізації.

Отримані результати дозволяють сформулювати умови, які послаблюють стійкість КГГ з нерівномірним рухом відносно запропонованої статистичної атаки. Зазначені умови полягають в тому, що коефіцієнти Уолша-Адамара комбінувальної функції генератора приймають нульові значення на всіх векторах ваги 0 і 1 та ненульові значення на певних векторах ваги 2. Показано, що ці умови виконуються для генератора гами шифру Alpha1. При цьому середній обсяг матеріалу, потрібного для відновлення початкового стану довільного КГГ, який задовольняє наведені умови, є за порядком таким самим, що і для шифру Alpha1.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]. J. Golic', "Cryptanalysis of alleged A5 stream cipher", in *Proc. Advances in Cryptology – EUROCRYPT'97, Lecture Notes in Computer Science*, vol 1233. Springer, Berlin, Heidelberg, 1997, pp. 239-255, doi: https://doi.org/10.1007/3-540-69053-0_17.

[2]. N. Komninos, B. Honary, and M. Darnell, "An Efficient Stream Cipher Alpha1 for Mobile and Wireless Devices", in *Cryptography and Coding, Lecture Notes in Computer Science*, vol. 2260. Springer, Berlin, Heidelberg, 2001, pp. 294-300, doi: https://doi.org/10.1007/3-540-45325-3_25.

[3]. P. Ekdahl, and T. Johansson, "Another attack on A5/1", *IEEE Trans. Inf. Theory*, vol. 49, iss. 1, 2003, pp. 284-289, doi: https://doi.org/10.1109/tit.2002.806129.

[4]. A. Maximov, T. Johansson, and S. Babbage, "An Improved Correlation Attack on A5/1", in *Selected Areas in Cryptography – SAC 2004, Lecture Notes in Computer Science*, vol. 3357. Springer, Berlin, Heidelberg, 2004, pp. 1-18, doi: https://doi.org/10.1007/978-3-540-30564-4_1.

[5]. A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC", in *Fast Software Encryption*, Springer, Berlin, Heidelberg, 2001, pp. 1-18, doi: https://doi.org/10.1007/3-540-44706-7_1.

[6]. E. Biham, and O. Dunkelman, "Cryptanalysis of the A5/1 GSM Stream Cipher", in *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2000, pp. 43-51, doi: https://doi.org/10.1007/3-540-44495-5_5.

[7]. T. Gendrullis, M. Novotný, A. Rupp, "A Real-World Attack Breaking A5/1 within Hours", in *Cryptographic Hardware and Embedded Systems – CHES 2008, Lecture Notes in Computer Science*, vol 5154. Springer, Berlin, Heidelberg, 2008, pp. 266-282, doi: https://doi.org/10.1007/978-3-540-85053-3_17.

[8]. C.J. Mitchell, "Remarks on the security of the Alpha1 stream cipher", *Technical Report RHUL–MA–2001-8*, 2001. [Online]. Available: https://www.academia.edu/55846558/Remarks_on_the_security_of_the_Alpha1_stream_cipher. Accessed on: Apr. 7, 2025.

[9]. Y. Xu, Y. Hao, and M. Wang, "Revisit Two Memoryless State-Recovery Cryptanalysis Methods on A5/1", Cryptology ePrint Archive, Paper 2023/1557. [Online]. Available:

https://ia.cr/2023/1557. Accessed on: Apr. 7, 2025.

[10]. А.М. Олексійчук, та А.А. Матійко, "Аналітичний вираз імовірності збігу сусідніх знаків вихідної послідовності комбінувального генератора гами, побудованого на базі регістрів зсуву, що рухаються з простоюванням", *Кібернетика та системний аналіз*, т. 61, № 2, с. 27-32, 2025, doi: https://doi.org/10.34229/KCA2522-9664.25.2.3.

[11]. А.М. Олексійчук, та Р.В. Проскуровський, "Нижня межа ймовірності розрізнення внутрішніх станів комбінувального генератора гами з нерівномірним рухом", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 2(13), с. 159-169, 2006.

[12]. Р.В. Проскуровський, "Аналітичні оцінки ефективності статистичного методу криптоаналізу комбінувального генератора гами з нерівномірним рухом", *Збірник наук. праць ВІТІ НТУУ "КПІ"*, № 1, с. 65-74, 2006.

[13]. А.М. Олексійчук, Р.В. Проскуровський, та А.С. Шевцов, "Аналітичні оцінки та достатні умови стійкості блокових шифрів та комбінувальних генераторів гами з нерівномірним рухом відносно статистичних методів криптоаналізу", *Прикладна радіоелектроніка*, т. 6, № 2, с. 264-273, 2007.

[14]. А.М. Олексійчук, та Р.В. Проскуровський, "Оцінка середньої ймовірності помилки байєсівського критерію для перевірки гіпотез в задачі криптоаналізу комбінувального генератора гами з нерівномірним рухом", *Теорія ймовірностей та математична статистика*, вип. 78, с. 152-159, 2008.

[15]. H. Wu, "Cryptanalysis of Stream Cipher Alpha1", in *Information Security and Privacy*, Springer, Berlin, Heidelberg, 2002, pp. 169-175, doi: https://doi.org/10.1007/3-540-45450-0_14.

[16]. K. Chen, L. Simpson, M. Henricksen, W. Millan and E. Dawson, "A Complete Divide and Conquer Attack on the Alpha1 Stream Cipher", in *Information Security and Cryptology – ICISC 2003*, Springer, Berlin, Heidelberg, 2004, pp. 418-431, doi: https://doi.org/10.1007/978-3-540-24691-6_31.

[17]. А.М. Олексійчук, та О.В. Курінний, *Методи криптоаналізу потокових шифрів. Навчальне видання.* Київ, Україна: КПІ ім. Ігоря Сікорського, 2023. [Електронний ресурс]. Доступно: https://ela.kpi.ua/server/api/core/bitstreams/a16bc1db-07a3-4d38-b9e7-a331ef2cc111/content. Дата звернення: Квіт. 7, 2025.

Стаття надійшла 14.04.2025.

REFERENCES:

[1]. J. Golic', "Cryptanalysis of alleged A5 stream cipher", in *Proc. Advances in Cryptology – EUROCRYPT'97, Lecture Notes in Computer Science*, vol 1233. Springer, Berlin, Heidelberg, 1997, pp. 239-255, doi: https://doi.org/10.1007/3-540-69053-0_17.

[2]. N. Komninos, B. Honary, and M. Darnell, "An Efficient Stream Cipher Alpha1 for Mobile and Wireless Devices", in *Cryptography and Coding, Lecture Notes in Computer Science*, vol. 2260. Springer, Berlin, Heidelberg, 2001, pp. 294-300, doi: https://doi.org/10.1007/3-540-45325-3_25.

[3]. P. Ekdahl, and T. Johansson, "Another attack on A5/1", *IEEE Trans. Inf. Theory*, vol. 49, iss. 1, 2003, pp. 284-289, doi: https://doi.org/10.1109/tit.2002.806129.

[4]. A. Maximov, T. Johansson, and S. Babbage, "An Improved Correlation Attack on A5/1", in *Selected Areas in Cryptography – SAC 2004, Lecture Notes in Computer Science*, vol. 3357. Springer, Berlin, Heidelberg, 2004, pp. 1-18, doi: https://doi.org/10.1007/978-3-540-30564-

4_1.

[5]. A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC", in *Fast Software Encryption*, Springer, Berlin, Heidelberg, 2001, pp. 1-18, doi: https://doi.org/10.1007/3-540-44706-7_1.

[6]. E. Biham, and O. Dunkelman, "Cryptanalysis of the A5/1 GSM Stream Cipher", in *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2000, pp. 43-51, doi: https://doi.org/10.1007/3-540-44495-5_5.

[7]. T. Gendrullis, M. Novotný, A. Rupp, "A Real-World Attack Breaking A5/1 within Hours", in *Cryptographic Hardware and Embedded Systems – CHES 2008, Lecture Notes in Computer Science*, vol 5154. Springer, Berlin, Heidelberg, 2008, pp. 266-282, doi: https://doi.org/10.1007/978-3-540-85053-3_17.

[8]. C.J. Mitchell, "Remarks on the security of the Alpha1 stream cipher", *Technical Report RHUL–MA–2001-8,* 2001. [Online]. Available: https://www.academia.edu/55846558/Remarks_on_the_security_of_the_Alpha1_stream_cipher. Accessed on: Apr. 7, 2025.

[9]. Y. Xu, Y. Hao, and M. Wang, "Revisit Two Memoryless State-Recovery Cryptanalysis Methods on A5/1", Cryptology ePrint Archive, Paper 2023/1557. [Online]. Available: https://ia.cr/2023/1557. Accessed on: Apr. 7, 2025.

[10]. A. Alekseychuk, and A. Matiyko, "Analytical expression of the probability of coincidence of adjacent signs of the output sequence of a combinational gamma generator built on the basis of shift registers moving with idle", *Cybernetics and Systems Analysis*, vol. 61, iss. 2, pp. 27-32, 2025, doi: https://doi.org/10.34229/KCA2522-9664.25.2.3.

[11]. A. Alekseychuk, and R. Proskurovsky, "Lower bound of probability of distinguishing internal states of a combinatorial gamma generator with non-uniform motion", *Legal, normative and metrological support of the information protection system in Ukraine*, iss. 2(13), pp. 159-169, 2006.

[12]. R. Proskurovsky, "Analytical evaluations of the effectiveness of the statistical method of cryptanalysis of a combinatorial gamma generator with non-uniform motion", *Coll. of scien. pap. of MITI NTUU "KPI"*, no. 1, pp. 65-74, 2006.

[13]. A. Alekseychuk, R. Proskurovsky, and A. Shevtsov, "Analytical estimates and sufficient conditions for the stability of block ciphers and combinational gamma generators with non-uniform motion with respect to statistical cryptanalysis methods", *Applied Radio Electronics*, vol. 6, iss. 2, pp. 264-273, 2007.

[14]. A. Alekseychuk, and R. Proskurovsky, "Estimation of the average error probability of the Bayesian criterion for hypothesis testing in the cryptanalysis problem of a combinatorial gamma generator with non-uniform motion", *Probability Theory and Mathematical Statistics*, iss. 78, pp. 152-159, 2008.

[15]. H. Wu, "Cryptanalysis of Stream Cipher Alpha1", in *Information Security and Privacy*, Springer, Berlin, Heidelberg, 2002, pp. 169-175, doi: https://doi.org/10.1007/3-540-45450-0_14.

[16]. K. Chen, L. Simpson, M. Henricksen, W. Millan and E. Dawson, "A Complete Divide and Conquer Attack on the Alpha1 Stream Cipher", in *Information Security and Cryptology – ICISC 2003*, Springer, Berlin, Heidelberg, 2004, pp. 418-431, doi: https://doi.org/10.1007/978-3-540-24691-6_31.

[17]. A. Alekseychuk, and O. Kurinnyi, *Methods of cryptanalysis of stream ciphers. Educational edition*. Kyiv, Ukraine: Igor Sikorsky Kyiv Polytechnic Institute, 2023. [Online]. Available: https://ela.kpi.ua/server/api/core/bitstreams/a16bc1db-07a3-4d38-b9e7-a331ef2cc111/content. Accessed on: Apr. 7, 2025.

ALEXANDRA MATIYKO,
ANTON ALEKSEYCHUK

A STATISTICAL ATTACK ON COMBINATION KEYSTREAM GENERATORS WITH IRREGULAR CLOCKING

Combination keystream generators with irregular clocking are the basis for constructing of stream ciphers, the most famous of which are A5 and Alpha1. Each such generator consists of several binary linear feedback shift registers, a Boolean combination function, and a register clocking control unit that defines the rules by which registers are shifted in the process of keystream generating. Despite certain weaknesses of known stream ciphers based on combination keystream generators with irregular clocking, such generators still arouse theoretical and applied interest due to the simplicity of their structure and the potential ability to provide security to a wide class of attacks, provided that their components are properly selected.

Combination keystream generators, each register of which is either shifted by one step or is idle in each clock cycle, with one of the registers clocking regularly, are investigated in the article. Previously, the authors of the article showed that the mentioned generators have an inherent weakness, which consists in statistical dependence between each neighboring signs of their output sequences. The main result of this article is a statistical attack based on the mentioned weakness. The proposed attack is aimed at restoring the initial state of the register clocking uniformly by a known output sequence of the generator or several such sequences produced by the generator in the chosen IV mode. It is shown that in the latter case the complexity of the attack depends linearly on the length of the mentioned register. An analytical bound of the amount of keystream required to implement the proposed attack with the required success probability is obtained. In particular, it is shown that for Alpha1 the corresponding amount is approximately 300 keystream frames along with their corresponding initialization vectors. Conditions that weaken the security of generators with irregular clocking against the proposed attack are formulated. They consist in the fact that the Walsh-Hadamard coefficients of the combination function take zero values on all vectors of weight 0 or 1 and non-zero values on certain vectors of weight 2. It is shown that these conditions are fulfilled for the keystream generator of Alpha1. In this case, the average amount of keystream required to recover the initial state of an arbitrary keystream generator that satisfies the above conditions is of the same order as for Alpha1.

Keywords: cryptographic information protection, combination keystream generators with irregular clocking, statistical attack, Walsh-Hadamard transform, A5/1, Alpha1.

Матійко Александра Андріївна, PhD, викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-6947-5958, alexm1710@ukr.net.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-4385-4631, alex-dtn@ukr.net.

Matiyko Alexandra, PhD, lecturer at the state information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Alekseychuk Anton, doctor of technical science, professor, professor at the state information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.