УДК 004.056:519.2 **DOI:10.30837/rt.2024.3.218.07**

А.М. ОЛЕКСІЙЧУК, д-р техн. наук, І.В. САМОЙЛОВ, канд. техн. наук

ЙМОВІРНІСНІ ВЛАСТИВОСТІ РОЗВ'ЯЗКІВ СИСТЕМ РІВНЯНЬ ГАМОУТВОРЕННЯ ГЕНЕРАТОРІВ ГАМИ З НЕРІВНОМІРНИМ РУХОМ

Вступ

Традиційною основою для побудови сучасних потокових шифрів є генератори гами, які базуються на лінійних регістрах зсуву (ЛРЗ) та нелінійних елементах ускладнення. Одним з відомих методів підвищення стійкості таких генераторів до алгебраїчних та кореляційних атак, є введення нерівномірності в процес руху ЛРЗ. Зазвичай нерівномірність руху забезпечується одним із двох способів: шляхом зовнішнього управління рухом або шляхом самоуправління, тобто встановлення детермінованої залежності кількості зсувів ЛЗР генератора в кожному такті від його поточного стану (див., наприклад [1, 2]).

Найвідоміші на сьогодні генератори гами з нерівномірним рухом, які застосовуються у потокових шифрах A5/1 [3], Alpha1 [4], LILI-128 [5] та деяких інших, ретельно досліджено ще у дев'яності та нульові роки. Проте інтерес фахівців до таких генераторів зберігається і сьогодні, про що свідчать нещодавні публікації [6, 7], присвячені новим атакам на шифр A5/1 та деякі інші потокові шифри, побудовані на базі генераторів гами з нерівномірним рухом.

Відомо, що за певних загальних умов нерівномірність руху ЛРЗ покращує криптографічні властивості генератора, збільшує значення періодів та еквівалентних лінійних складностей його вихідних послідовностей, підвищує його стійкість відносно кореляційних атак [8, 9]. Проте відомі методи оцінювання стійкості генераторів гами з нерівномірним рухом, розвинуті переважно в дев'яності роки [8 – 13], базуються на спрощеному описі їх функціонування. З одного боку, це надає змогу охопити широкий клас різноманітних генераторів гами, але, з іншого – знижує точність та адекватність висновків про стійкість окремих з них. Як приклад, відзначимо генератори з векторним зовнішнім управлінням рухом, які являють собою багатовимірне узагальнення найбільш дослідженого класу ЛРЗ з нерівномірним рухом, до якого відносяться генератори гами потокових шифрів A5/1 та Alpha1.

Мета статті – дослідити ймовірнісні властивості розв'язків системи рівнянь (СР) гамоутворення довільних та комбінувальних, генераторів гами з нерівномірним рухом.

В п. 1 наведено загальну ймовірнісну модель, яка описує функціонування таких генераторів [2].

В п. 2 за допомогою теоретико-автоматних методів отримано матричне представлення для середнього числа розв'язків СР гамоутворення генератора гами з нерівномірним рухом. Встановлено умови, за яких комбінувальний генератор із зовнішнім управлінням є необоротним за Гаффманом, а також достатні умови експоненційного росту середнього числа розв'язків системи гамоутворення цього генератора від довжини його вихідної послідовності.

В п. 3 отримано аналітичні вирази та оцінки розподілів ймовірностей сум випадкових векторів, які виробляються блоками управління рухом певного класу комбінувальних генераторів гами.

1. Ймовірнісна модель генератора гами з нерівномірним рухом

За означенням генератор гами являє собою скінченний автономний автомат $\Im = (S, Y, h, f)$, де S та Y позначають відповідно внутрішній та вихідний алфавіти автомата $\Im$, $h: S \to S$ і $f: S \to Y$ є відповідно функціями переходів та виходів цього автомата (див., наприклад, [1, 2]).

Позначимо $x(0) \in S$ початковий стан автомата $\Im$, $\bar{x} = \{x(i) : i = 0,1, ...\}$ – його внутрішню послідовність,

$$x(i) = h^i(x(0)),\ i = 0,1, \ldots . \tag{1}$$

Нехай, далі, (A, p_A) – дискретне джерело без пам'яті, де $A \subseteq \mathbf{N}_0$, p_A – розподіл ймовірностей на множині A. Джерело виробляє послідовність незалежних випадкових величин (ВВ) $\varepsilon(0), \varepsilon(1), \ldots$, кожна з яких розподілена на множині A за законом p_A:

$$\mathbf{P}(\varepsilon(i) = a) = p_A(a),\ a \in A,\ i = 0,1, \ldots .$$

Розглянемо ВВ $\delta(0) \equiv 0$, $\delta(i) = \varepsilon(0) + \ldots + \varepsilon(i-1)$, $i = 0,1, \ldots$, та визначимо таку послідовність знаків алфавіту *Y*, що відповідає послідовностям (1) і $\bar{\delta} = \{\delta(i) : i = 0,1,...\}$:

$$y(i) = f(x(\delta(i))),\ i = 0,1,\ldots . \tag{2}$$

Відзначимо, що $\bar{y} = \{y(i) : i = 0,1,\ldots\}$ є випадковою послідовністю, яка залежить від $\bar{\delta}$ та початкового стану $x(0)$ автомата $\Im$. Надалі вважатимемо, що $x(0)$ є випадковим елементом, який не залежить від $\bar{\delta}$ та має рівномірний розподіл ймовірностей на множині S.

Співвідношення (1), (2) (разом із зазначеними вище обмеженнями щодо законів розподілу ВВ $x(0)$ та $\delta(i)$, $i = 0,1, \ldots$) являють собою загальну ймовірнісну модель генератору гами з нерівномірним рухом [2].

Зазвичай на практиці в ролі джерела (A, p_A) використовується деякий автономний автомат, що виробляє послідовність $\varepsilon(0), \varepsilon(1), \ldots$ невід'ємних цілих чисел. Такий автомат називають блоком управління рухом генератора гами $\Im$. Як додаткове припущення часто приймають таку умову: $x(0), x(1), \ldots$ є послідовністю незалежних ВВ, що рівномірно розподілені на множині S. Іншими словами, замість псевдовипадкової послідовності (1) розглядають випадкову послідовність $\{x(i) : i = 0,1, ...\}$, знаки якої є незалежними рівномірно розподіленими на множині S випадковими величинами.

Надалі вважатимемо, що $p_A(a) > 0$ для кожного $a \in A$. В цьому випадку генератор гами, функціонування якого описується співвідношеннями (1) і (2), називається генератором гами з A-рухом. Говорять про обмежений A-рух, якщо $|A| < \infty$, та необмежений A-рух – у протилежному випадку [9, 11].

Приклад 1. Нехай $\Im = (S, Y, h, f)$ – регістр зсуву довжини n з лінійним зворотним зв'язком та функцією ускладнення $f = f(x_1, ..., x_n)$, де $S = V_n = \{0,1\}^n$, $Y = \{0,1\}$. Позначимо $m(x) = x^n \oplus c_{n-1}x^{n-1} \oplus ... \oplus c_0$, де $c_i \in Y$, $i \in \overline{0,\ n-1}$, поліном зворотного зв'язку регістра, U – його супровідну матрицю. Тоді стан $x(i) = (x_0(i), \ldots, x_{n-1}(i))$ регістра $\Im$ в i-му такті визначається за формулою $x(i) = x(0)U^i$, $i = 0,1, \ldots$.

Нехай, далі, $i_1, ..., i_k$ – номери точок знімання інформації з накопичувача регістра зсуву на входи функції f, $0 \le i_1 < ... < i_k \le n-1$, $\prod$ – $(n \times k)$-матриця, j-й стовпець якої має єдину одиницю в j-му рядку $(j \in \overline{1,k})$ та нулі в інших рядках. Тоді знак вихідної послідовності регістра $\Im$ в i-му такті дорівнює $f(x(0)U^i \prod)$, $i = 0,1, \ldots$. Якщо (A, p_A) – блок управління рухом регістра $\Im$, то він виробляє знаки двійкової послідовності $y(i) = f(x(0)U^{\delta(i)} \prod)$, $i = 0,1,\ldots$, де $\delta(0) \equiv 0$, $\delta(i) = \varepsilon(0) + ... + \varepsilon(i-1)$, $\varepsilon(i)$ – незалежні випадкові величини, що розподілені на множині A за законом p_A, $i = 0,1, \ldots$.

Відзначимо, що у більшості публікацій досліджуються властивості найпростішого класу лінійних регістрів зсуву з нерівномірним рухом, які характеризуються умовами $k = 1$, $f(x_1) = x_1$, $x_1 \in \{0,1\}$.

Приклад 2. Розглянемо більш загальний варіант управління рухом автономного автомата $\Im$, що є каскадом паралельного з'єднання n автономних автоматів без виходу та автомата без пам'яті [2].

Нехай $S = V_{L_1} \times ... \times V_{L_n}$, $\Im = (S, Y, h, f)$ – автономний автомат з функцією переходів

$$h(z_1, ..., z_n) = (h_1(z_1), ..., h_n(z_n)), \quad z_j \in V_{L_j}, \ j \in \overline{1, n}, \tag{3}$$

де $h_j : V_{L_j} \to V_{L_j}$, $j \in \overline{1, n}$. Нехай, далі,

$$(x_1(i), ..., x_n(i)) = (h_1^i(x_1(0)), ..., h_n^i(x_n(0))), \ i = 0, 1, ... \tag{4}$$

внутрішня послідовність автомата $\Im$, що відповідає його початковому стану $(x_1(0), \ ..., x_n(0))$.

Припустимо, що $A \subseteq \mathbf{N}_0^n$, а $\varepsilon(i) = (\varepsilon_1(i), ..., \varepsilon_n(i))$ є n-вимірним випадковим вектором, розподіленим на множині A за законом p_A, $i = 0, 1, \ ...$. Позначимо $\delta(0) \equiv 0$, $\delta(i) = (\delta_1(i), ..., \delta_n(i)) = \varepsilon(0) + ... + \varepsilon(i-1)$, $i = 0, 1, \ ...$ та задамо випадкову послідовність

$$y(i) = f(x_1(\delta_1(i)), ..., x_n(\delta_n(i))), \ i = 0, 1, ... \tag{5}$$

Співвідношення (4), (5) являють собою n-вимірне узагальнення співвідношень (1), (2). Назвемо генератор, який функціонує за законами (4), (5), генератором гами з векторним зовнішнім управлінням. Конкретним прикладом такого генератора є комбінувальний генератор гами з нерівномірним рухом [1, 2].

2. Теоретико-автоматний підхід до аналізу криптографічних властивостей генераторів гами з нерівномірним рухом

Нехай $\Im = (S, Y, h, f)$ – довільний автономний автомат, (A, p_A) – блок управління його рухом, де $A \subseteq \mathbf{N}_0$, $|A| < \infty$, p_A – рівномірний розподіл ймовірностей на множині A.

Задамо новий автомат $\Im_A = (A, S, Y, h_A, f_A)$ із вхідним алфавітом A та функціями переходів і виходів

$$h_A(x, \varepsilon) = h^{\varepsilon}(x), \ x \in S, \ \varepsilon \in A, \tag{6}$$

$$f_A(x, \varepsilon) = f(x), \ x \in S, \ \varepsilon \in A \tag{7}$$

відповідно. Зрозуміло, що, за умови фіксації початкового стану $x(0)$ автомата $\Im_A$, він переробляє довільну вхідну послідовність $\varepsilon(0), \varepsilon(1), ..., \varepsilon(t-1)$, $t \in \mathbf{N}$, у вихідну послідовність $f(x(0)), f(x(\delta(1))), ..., f(x(\delta(t)))$, яка співпадає з початковим фрагментом вихідної послідовності генератора гами з нерівномірним рухом, що функціонує за законами (1), (2). Отже, цей генератор можна розглядати як скінченний автомат $\Im_A$, який перетворює вхідні послідовності, що виробляються блоком управління рухом автомата $\Im$, у вихідні послідовності вигляду (2).

Зазначена інтерпретація процесу функціонування генератора гами з нерівномірним рухом надає змогу безпосередньо застосовувати до аналізу його криптографічних властивостей відомі теоретико-автоматні методи. Задача відновлення початкового стану генератора гами з нерівномірним рухом за його вихідною послідовністю зводиться до однієї зі стандартних загальних задач теорії автоматів: відновлення початкового стану скінченного автомату за відомим виходом при невідомому вході (але відомому розподілі ймовірностей на вхідному алфавіті) [14].

Зауважимо, що система рівнянь гамоутворення генератора $\Im_A$ у тактах з номерами $1, 2, ..., t$ має такий вигляд:

$$
\begin{aligned}
f(h^{\varepsilon(0)}(x(0))) &= y(1),\\
\dots \quad \dots \quad \dots \quad &\dots\\
f(h^{\varepsilon(0)+\dots+\varepsilon(i-1)}(x(0))) &= y(i),\\
\dots \quad \dots \quad \dots \quad &\dots\\
f(h^{\varepsilon(0)+\dots+\varepsilon(t-1)}(x(0))) &= y(t),
\end{aligned}
\tag{8}
$$

де $x(0)$ та $(\varepsilon(0),\dots,\varepsilon(t-1))$ є відповідно невідомий початковий стан та невідома вхідна послідовність автомата $\Im_A$, $\bar{y}=(y(1),\dots,y(t))$ – його відома вихідна послідовність.

Позначимо $\eta_t(\bar{y})$ число розв'язків $(x(0),\varepsilon(0),\dots,\varepsilon(t-1))$ системи рівнянь (8). Зауважимо, що, згідно з припущеннями з п. 1 $\eta_t(\bar{y})$ є випадковою величиною, розподіл якої характеризує, зокрема, обчислювальну складність відновлення початкового стану $x(0)$ автомата $\Im_A$ за фрагментом його вихідної послідовності $\bar{y}$ шляхом повного перебору всіх можливих розв'язків системи (8). Це відноситься також і до більш загального варіанту зовнішнього управління рухом автомата $\Im$, коли $A\subseteq \mathbf{N}_0^n$ (див. приклад 2).

Відомо [14], що характер асимптотичної поведінки розподілу ВВ $\eta_t(\bar{y})$ при $t\to\infty$ залежить від того, чи володіє автомат $\Im_A$ властивістю оборотності за Гаффманом. Нагадаємо (див., наприклад, [2]), що автомат $\Im_A$ називається необоротним за Гаффманом, якщо існують стан $x_1\in S$ та вхідні послідовності $\varepsilon_1,\dots,\varepsilon_k$ і $\varepsilon_1',\dots,\varepsilon_k'$, де $k\ge 3$, такі, що

(*а*) $(x_1,\varepsilon_1)=(x_1,\varepsilon_1')$, $(x_k,\varepsilon_k)=(x_k',\varepsilon_k')$;

(*б*) $(\varepsilon_2,\dots,\varepsilon_{k-1})\ne(\varepsilon_2',\dots,\varepsilon_{k-1}')$;

(*в*) $f(x_i,\varepsilon_i)=f(x_i',\varepsilon_i')$, $i\in\overline{1,k}$,

де x_i, x_i' визначаються рекурентно за формулами $x_{i+1}=h^{\varepsilon_i}(x_i)$, $x_{i+1}'=h^{\varepsilon_i'}(x_i')$, $i\in\overline{1,k-1}$.

З результатів [14] випливає, що у випадку, коли автомат $\Im_A$ є оборотним за Гаффманом, значення випадкової величини $\eta_t(\bar{y})$ обмежені зверху певною константою, яка не залежить від $t\in\mathbf{N}$. Навпаки, для необоротного за Гаффманом автомата $\Im_A$ (за певних загальних умов) значення $\eta_t(\bar{y})$ експоненційно зростає при $t\to\infty$ для більшості вихідних послідовностей $\bar{y}=(y(1),\dots,y(t))$.

Як приклад, розглянемо комбінувальний генератор $\Im$, який складається з n лінійних регістрів зсуву та функції ускладнення $f:V_n\to\{0,1\}$. Нехай (A,p_A) – блок управління рухом цього генератора, де $A\subseteq\mathbf{N}_0^n$, $\Im_A$ – скінченний автомат, який йому відповідає.

Твердження 1. Нехай існують вектори $b=(b_1,\dots,b_n)$, $c=(c_1,\dots,c_n)\in A$, $b\ne c$, такі, що всі координати вектора $b+c$ не перевищують довжину найкоротшого регістра зсуву комбінувального генератора $\Im$. Тоді автомат $\Im_A$ є необоротним за Гаффманом.

Доведення. Позначимо $x_j=(x_j(0),\dots,x_j(L_j-1))$ початковий стан j-го регістра генератора $\Im$, $j\in\overline{1,n}$. Розглянемо вхідні послідовності

$$\varepsilon_1=a,\ \varepsilon_2=b,\ \varepsilon_3=c, \tag{9}$$

$$\varepsilon_1'=a,\ \varepsilon_2'=c,\ \varepsilon_3'=b, \tag{10}$$

де $a=(a_1,...,\ a_n)$ – довільний елемент множини *A*. Знаки вихідних послідовностей автомата $\Im_A$ у тактах 0, 1, 2, 3, що відповідають послідовностям (9) та (10), дорівнюють відповідно

$$f(x_1(0),...,x_n(0)),\ f(x_1(a_1),...,x_n(a_n)),\ f(x_1(a_1+b_1),...,x_n(a_n+b_n)),$$
$$f(x_1(a_1+b_1+c_1),...,x_n(a_n+b_n+c_n)) \tag{11}$$

та

$$f(x_1(0),...,x_n(0)),\ f(x_1(a_1),...,x_n(a_n)),\ f(x_1(a_1+c_1),...,x_n(a_n+c_n)),$$
$$f(x_1(a_1+b_1+c_1),...,x_n(a_n+b_n+c_n)). \tag{12}$$

Нехай $(\alpha_1,...,\ \alpha_n)\in V_n$ – довільний вектор такий, що $f(\alpha_1,...,\ \alpha_n)=0$. Тоді за умови твердження можна вибрати початковий стан автомата $\Im_A$ таким чином, щоб виконувалися рівності

$$x_1(a_1+b_1)=x_1(a_1+c_1)=\alpha_1,\ \ldots,\ x_n(a_n+b_n)=x_n(a_n+c_n)=\alpha_n. \tag{13}$$

Безпосередньо з формул (11) – (13) випливає, що вхідні послідовності (9), (10) та вибраний початковий стан автомата $\Im_A$ задовольняють умови (*а*) – (*в*). Отже, автомат $\Im_A$ є необоротним за Гаффманом, що й треба було довести.

Кажучи неформально, отримане твердження показує, що з ростом довжини вихідної послідовності комбінувального генератора гами з нерівномірним рухом число її прообразів, тобто відповідних розв'язків системи рівнянь (8), майже завжди зростає експоненційно швидко.

Більш точні результати про асимптотичну поведінку числа прообразів вихідних послідовностей скінченних автоматів викладено в [14]. Як правило, спроби застосування зазначених результатів до конкретних генераторів з нерівномірним рухом, які використовуються на практиці, пов'язані зі значними аналітичними труднощами. Відмітимо, що навіть для "простішого" випадку ЛРЗ з *A*-рухом, де $|A|=2$, задача отримання аналітичного виразу закону розподілу ВВ $\eta_t(\bar{y})$ залишається дуже складною та є далекою від повного вирішення [9, 11].

Певну (але неповну) інформацію про характер росту типових значень $\eta_t(\bar{y})$ як функції параметру *t* надає залежність від *t* середнього числа розв'язків СР (8), тобто математичного сподівання $\mathbf{E}\eta_t(\bar{y})$ [14].

Наступне твердження показує, що для широкого класу генераторів гами з нерівномірним рухом асимптотична поведінка параметра $\mathbf{E}\eta_t(\bar{y})$ при $t\to\infty$ визначається властивостями послідовності степенів деякої $(0,1)$-матриці, яка відповідає автомату $\Im_A$.

Твердження 2. Нехай автомат $\Im_A = (A,S,Y,h_A,f_A)$ задовольняє таку властивість: для довільних $x,\ x'\in S$ існує не більш одного $\varepsilon\in A$ такого, що $h_A(x,\varepsilon)=x'$. Задамо орієнтований граф $\Delta(\Im_A)$ з множиною вершин $S\times S$, в якому для кожної пари вершин (x_1,x_1'), (x_2,x_2') дуга, що спрямована з (x_1,x_1') до (x_2,x_2'), існує тоді й тільки тоді, коли для деяких $\varepsilon,\varepsilon'\in A$ виконуються умови

$$x_2=h^{\varepsilon}(x_1),\ x_2'=h^{\varepsilon'}(x_1'),\ f(x_2)=f(x_2'). \tag{14}$$

Позначимо $D(\Im_A)$ матрицю суміжності орграфу $\Delta(\Im_A)$. Тоді для кожного $t\in\mathbf{N}$ має місце рівність

$$\mathbf{E}\eta_t(\bar{y})=\frac{1}{|A|^t|S|}\omega(D(\Im_A)^t), \tag{15}$$

де $\omega(\cdot)$ позначає вагу (суму всіх елементів) відповідної матриці.

Доведення. Для будь-яких $t \in \mathbf{N}$, $x,\ x' \in S$ та $\bar{y} \in Y^t$ позначимо $C_{\bar{y}}(x, x')$ число розв'язків $(x(0), \varepsilon(0), \ldots, \varepsilon(t-1))$ системи рівнянь (8) таких, що $x(0) = x$, $h^{\varepsilon(0)+\ldots+\varepsilon(t-1)}(x(0)) = x'$.

Розглянемо матриці $C_{\bar{y}}$ та $D_{\bar{y}}$ порядків $|S|$ та $|S|^2$ з елементами

$$C_{\bar{y}}(x, x'),\ x,\ x' \in S$$

та

$$D_{\bar{y}}((x_1, x_1'), (x_2, x_2')) = C_{\bar{y}}(x_1, x_2) C_{\bar{y}}(x_1', x_2'),\ (x_1, x_1'),\ (x_2, x_2') \in S^2 \tag{16}$$

відповідно. За умови твердження при $t = 1$ виконуються такі умови:

$C_y(x, x') = 1$, якщо існує (єдиний) $\varepsilon \in A$ такий, що $h_A(x, \varepsilon) = x'$, $f(x') = y$;

$C_y(x, x') = 0$ – у протилежному випадку,

де $x,\ x' \in S$, $y \in Y$. Отже, згідно з формулами (14), (16) маємо

$$D(\Im_A) = \sum_{y \in Y} D_y . \tag{17}$$

Далі, для кожного $\bar{y} = (y(1), \ldots, y(t)) \in Y^t$, де $t \in \mathbf{N}$, виконується рівність

$$C_{\bar{y}} = C_{y(1)} \cdots C_{y(t)}, \tag{18}$$

яка, у свою чергу, тягне рівність

$$D_{\bar{y}} = D_{y(1)} \cdots D_{y(t)} . \tag{19}$$

Таким чином, внаслідок формули (18) маємо

$$\eta_t(\bar{y}) = \sum_{(x,x') \in S^2} C_{\bar{y}}(x, x') = \omega(C_{y(1)} \cdots C_{y(t)}),\ \bar{y} = (y(1), \ldots, y(t)) \in Y^t . \tag{20}$$

Для доведення формули (15), скористуємося рівністю [14]

$$\mathbf{E}\eta_t(\bar{y}) = \frac{1}{|A|^t |S|} \sum_{\bar{y} \in Y^t} \eta_t(\bar{y})^2 . \tag{21}$$

Підставляючи вираз (20) у формулу (21) та послідовно використовуючи рівності (16), (19), (17), отримаємо такі співвідношення:

$$\mathbf{E}\eta_t(\bar{y}) = \frac{1}{|A|^t |S|} \sum_{\bar{y} \in Y^t} (\omega(C_{y(1)} \cdots C_{y(t)}))^2 = \frac{1}{|A|^t |S|} \sum_{\substack{(x_1, x_2) \in S^2,\\ (x_1', x_2') \in S^2}} \sum_{\bar{y} \in Y^t} C_{\bar{y}}(x_1, x_2) C_{\bar{y}}(x_1', x_2') =$$

$$= \frac{1}{|A|^t |S|} \sum_{\substack{(x_1, x_2) \in S^2,\\ (x_1', x_2') \in S^2}} \sum_{\bar{y} \in Y^t} D_{\bar{y}}((x_1, x_1'), (x_2, x_2')) = \frac{1}{|A|^t |S|} \omega\left(\sum_{\bar{y} = (y(1), \ldots, y(t)) \in Y^t} D_{y(1)} \cdots D_{y(t)} \right) =$$

$$= \frac{1}{|A|^t |S|} \omega\left(\left(\sum_{y \in Y} D_y \right)^t \right) = \frac{1}{|A|^t |S|} \omega(D(\Im_A)^t) .$$

Твердження доведено.

Зауважимо, що формули (18), (20) та (21) надають змогу встановити прості аналітичні вирази меж параметра $\mathbf{E}\eta_t(\bar{y})$ для різноманітних генераторів гами з нерівномірним рухом. У певних випадках такі межі містять явну інформацію про експоненційну швидкість зростання середнього числа розв'язків СР (8) від параметра t, тобто довжини вихідної послідовності генератора гами.

Як приклад, наведемо твердження, яке є безпосереднім наслідком попереднього та встановлює аналітичні межі середнього числа розв'язків СР гамоутворення комбінувального генератора гами з нерівномірним рухом.

Твердження 3. Нехай $\Im_A$ – комбінувальний генератор з множиною станів S, яка складається з n ЛРЗ максимального періоду та зрівноваженої комбінувальної функції $f: V_n \to \{0, 1\}$, (A, p_A) – блок управління рухом цього генератора, де $|A| < \infty$, p_A – рівномірний розподіл ймовірностей на множині A.

Тоді для кожного $t \in \mathbf{N}$ виконується нерівності

$$1/2^t \,|S|\,|A|^t \le \mathbf{E}\eta_t(\bar{y}) \le 1/2\,|S|\,|A|^t. \tag{22}$$

Зауважимо, що згідно з оцінками (22) величина $|S|^{-1}\mathbf{E}\eta_t(\bar{y})$ експоненційно швидко прямує до нескінченності при $t \to \infty$ у випадку, коли $|A| > 2$.

3. Розподіли ймовірностей сум незалежних випадкових векторів, що виробляються блоками управління рухом генераторів гами

Важливою окремою задачею ймовірнісного аналізу системи рівнянь (8) є дослідження розподілів ймовірностей випадкових векторів $\delta(i) = \varepsilon(0) + ... + \varepsilon(i-1)$, які визначають сумарні величини зсувів регістрів даного генератора гами протягом i тактів, $i = 1, 2, ...$ (див. приклади 1, 2). До цієї задачі приводить, зокрема, аналіз ефективності кореляційних атак на різноманітні генератори гами з нерівномірним рухом [13, 15, 16].

Зауважимо, що, оскільки випадкові вектори $\varepsilon(i)$, $i = 1, 2, ...$, є незалежними у сукупності та однаково розподілені на множині $A \subseteq \mathbf{N}_0^n$ (яка звичайно є скінченною), то, за умови оборотності коваріаційної матриці K випадкового вектора $\varepsilon(0)$, граничний розподіл послідовності $\{\frac{1}{\sqrt{i}}(\delta(i) - i\mathbf{E}\varepsilon(0)) : i = 1, 2, ...\}$ є нормальним з параметрами $(0, K)$ (див., наприклад, [17, с. 174]). Проте, на практиці аналіз криптографічних властивостей генераторів гами з нерівномірним рухом, як правило, потребує неасимптотичних виразів або оцінок ймовірностей значень випадкових величин $\delta(i)$.

Нижче (за певних обмежень відносно блоку управління рухом заданого генератора гами) наведені такі вирази та оцінки.

Нехай $A = \{a_1, ..., a_m\} \subseteq \mathbf{N}_0^n$, $\{\varepsilon(i) : i = 0, 1, ...\}$ – послідовність незалежних випадкових векторів, що розподілені за законом $\mathbf{P}(\varepsilon(i) = a) = m^{-1}$, $a \in A$. Позначимо $\delta(0) \equiv 0$, $\delta(i) = \varepsilon(0) + ... + \varepsilon(i-1)$, $i = 1, 2, \ldots$, та отримаємо вираз розподілу ймовірностей випадкового вектора $\delta(i)$.

Зрозуміло, що

$$\mathbf{P}(\delta(i) = a) = m^{-i} \sum_{\substack{(\alpha_0, ..., \alpha_{i-1}) \in A^i: \\ \alpha_0 + ... + \alpha_{i-1} = a}} 1, \quad i = 1, 2, \ldots, \; a \in \mathbf{N}_0^n. \tag{23}$$

Розіб'ємо набори, за якими ведеться підсумування у формулі (23), на класи, що попарно не перетинаються, відносячи до того ж самого класу такі набори $(\alpha_0, ..., \alpha_{i-1})$, що мають одинакові вектори частот зустрічаємості $\mu_1, ..., \mu_m$ елементів $a_1, ..., a_m$ відповідно.

Помітимо, що для будь-яких $\mu_1, ..., \mu_m \in \mathbf{N}_0$, де $\mu_1 + ... + \mu_m = i$, існує точно $\frac{i!}{\mu_1! ... \mu_m!}$ наборів $(\alpha_0, ..., \alpha_{i-1}) \in A^i$ таких, що частота зустрічаємості елемента a_j в наборі $(\alpha_0, ..., \alpha_{i-1})$ дорівнює μ_j, $j \in \overline{1, m}$. Звідси внаслідок рівності (23) отримаємо, що

$$\mathbf{P}(\delta(i) = a) = m^{-i} \sum_{\substack{(\mu_1, ..., \mu_m) \in \mathbf{N}_0^m: \\ a_1\mu_1 + ... + a_m\mu_m = a, \\ \mu_1 + ... + \mu_m = i}} \frac{i!}{\mu_1! ... \mu_m!}, \quad i = 1, 2, ..., \ a \in \mathbf{N}_0^n. \tag{24}$$

Розглянемо окремий випадок, в якому елементи $a_1, ..., a_m$ множини A є лінійно незалежними (над полем $\mathbf{R}$) n-вимірними векторами. В цьому випадку для будь-якого $a \in \mathbf{N}_0^n$ існує єдиний набір чисел $\mu_1, ..., \mu_m$ такий, що $a = a_1\mu_1 + ... + a_m\mu_m$. Звідси внаслідок формули (24) випливає такий результат.

Твердження 4. Нехай $A = \{a_1, ..., a_m\} \subseteq \mathbf{N}_0^n$, де вектори $a_1, ..., a_m$ є лінійно незалежними над полем $\mathbf{R}$. Тоді для довільних $a \in \mathbf{N}_0^n$, $i = 1, 2, ...$ таких, що

$$a = a_1\mu_1 + ... + a_m\mu_m, \ i = \mu_1 + ... + \mu_m, \ \mu_j \in \mathbf{N}_0, \ j \in \overline{1, m}, \tag{25}$$

виконується рівність

$$\mathbf{P}(\delta(i) = a) = m^{-i} \frac{i!}{\mu_1! ... \mu_m!}. \tag{26}$$

Якщо ж a та i не можуть бути представлені у вигляді (25), то $\mathbf{P}(\delta(i) = a) = 0$.

Розглянемо зараз випадок, у якому вектори $a_1, ..., a_{m-1}$ є лінійно незалежними над полем $\mathbf{R}$, а вектор a_m дорівнює їхній лінійній комбінації з раціональними коефіцієнтами:

$$a_m = a_1c_1 + ... + a_{m-1}c_{m-1}, \ c_j \in \mathbf{Q}, \ j \in \overline{1, m-1}. \tag{27}$$

Покажемо, що за умови

$$c_1 + ... + c_{m-1} \neq 1 \tag{28}$$

сума (24) має не більше одного ненульового доданка, внаслідок чого виконується рівність (26).

Дійсно, припустимо, що існує два різних набори $(\mu_1, ..., \mu_m)$, $(\nu_1, ..., \nu_m) \in \mathbf{N}_0^m$ таких, що

$$\sum_{j=1}^{m} \mu_j a_j = \sum_{j=1}^{m} \nu_j a_j = a, \ \sum_{j=1}^{m} \mu_j = \sum_{j=1}^{m} \nu_j = i. \tag{29}$$

З першої рівності (29) маємо $\sum_{j=1}^{m-1} (\mu_j - \nu_j) a_j = (\nu_m - \mu_m) a_m$, звідки в силу лінійної незалежності векторів $a_1, ..., a_{m-1}$ випливає, що $\nu_m \neq \mu_m$ та

$$c_j = \frac{\mu_j - \nu_j}{\nu_m - \mu_m}, \ j \in \overline{1, m-1}. \tag{30}$$

Підсумовуючи рівності (30) за всіма $j \in \overline{1, m-1}$, знайдемо, що

$$\sum_{j=1}^{m-1} c_j = \frac{1}{\nu_m - \mu_m}\left(\sum_{j=1}^{m-1}\mu_j - \sum_{j=1}^{m-1}\nu_j\right) = \frac{i-\mu_m - i+\nu_m}{\nu_m-\mu_m} = 1.$$

Але це суперечить умові (28). Отже, сума (24) має не більше одного ненульового доданка, що й треба було довести.

Таким чином, отримано наступний результат.

Твердження 5. Нехай множина $A = \{a_1, ..., a_m\}$ задовольняє умови (27), (28), де вектори $a_1, \ldots, a_{m-1}$ є лінійно незалежними над полем $\mathbf{R}$. Тоді справджується висновок твердження 4.

Приклад 3. Нехай $m = n+1$, $A = \{a_1, ..., a_{n+1}\} \subseteq \mathbf{N}_0^n$,

$$a_i = (\beta, ..., \beta, \alpha, \beta, ..., \beta),\ i \in \overline{1, n},\ a_{n+1} = (\beta, ..., \beta), \tag{31}$$

де $\alpha, \beta \in \mathbf{N}_0, \alpha \neq \beta$. Неважко перевірити, що вектори $a_1, ..., a_{n+1}$ задовольняють умову твердження 5, де $a_{n+1} = \dfrac{\beta}{\alpha + (n-1)\beta}\sum_{j=1}^{n} a_j$, тобто $c_j = \dfrac{\beta}{\alpha+(n-1)\beta}$, $j \in \overline{1, n}$.

Отже, згідно з твердженням 5 для довільних $\mu_1, ..., \mu_m \in \mathbf{N}_0$ та a, i, що задовольняють умову (25), виконується рівність (26).

Зауважимо, що в окремому випадку $n = 3$, $\alpha = 0$, $\beta = 1$ співвідношення (31) описують блок (само)управління рухом генератора гами шифру A5/1.

Наведемо оцінки двійкового логарифму ймовірності (26) за умови (25).

Скористаємося відомими нерівностями (див., наприклад, [18]):

$$m^{-i}\frac{2^{iH(q_1,...,q_m)}}{\sqrt{(2\pi i)^{m-1} q_1 ... q_m}} \exp\left\{-\sum_{j=1}^{m}\frac{1}{12 i q_j}\right\} < \mathbf{P}(\delta(i) = a) < m^{-i}\frac{2^{iH(q_1,...,q_m)}}{\sqrt{(2\pi i)^{m-1} q_1 ... q_m}}, \tag{32}$$

де $q_j = \dfrac{\mu_j}{i}$, $j \in \overline{1, m}$, $H(q_1, ..., q_m) = -\sum_{j=1}^{m} q_j \log q_j$.

Нехай $\mu_j = t \in \mathbf{N}$ для всіх $j \in \overline{1, m}$, $a = t(a_1 + ... + a_m)$, $i = tm$. Тоді, на підставі формул (26), (32), отримаємо, що

$$\log \mathbf{P}(\delta(i) = a) < -\frac{1}{2}((m-1)\log(2\pi i) - m\log m),$$

$$\log \mathbf{P}(\delta(i) = a) > -\frac{1}{2}((m-1)\log(2\pi i) - m\log m) - \frac{1}{12i}\log e.$$

Отже, для будь-яких

$$a = t(a_1 + ... + a_m),\ i = tm,\ \ t = 1, 2, ... \tag{33}$$

виконується рівність

$$-\log \mathbf{P}(\delta(i) = a) = \frac{1}{2}(m-1)(\log t + \log(2\pi)) - \frac{1}{2}\log m + \Delta_{t,m}, \tag{34}$$

де $0 \le \Delta_{t,m} \le \dfrac{\log e}{12tm}$. Як видно з формул (33), (34), значення $\mathbf{P}(\delta(i) = a)$ прямують до нуля зі швидкістю порядку $O(t^{-1})$ при $t \to \infty$.

Висновки

Основними результатами статті є ймовірнісні властивості розв'язків систем рівнянь гамоутворення генераторів гами з нерівномірним рухом (див. вище твердження 1 – 5). Отримано матричне представлення для середнього числа розв'язків зазначених систем рівнянь та встановлено умови, за яких комбінувальний генератор із зовнішнім управлінням є необоротним за Гаффманом. Отримано достатні умови експоненційного росту середнього числа розв'язків системи гамоутворення цього генератора від довжини його вихідної послідовності, аналітичні вирази та оцінки розподілів ймовірностей сум випадкових векторів, які виробляються блоками управління рухом певного класу комбінувальних генераторів гами.

Результати можуть бути застосовані при розв'язанні задач оцінювання стійкості генераторів гами із зовнішнім управлінням рухом та обґрунтування вимог до криптографічних параметрів вузлів ускладнення таких генераторів гами, що визначають їхню стійкість відносно кореляційних атак.

Список літератури:

1. Katz J., Lindell Y. Introduction to Modern Cryptography. Taylor & Francis Group, 2021. 628 p.
2. Олексійчук А. М., Курінний О. В. Методи криптоаналізу потокових шифрів : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 172 с.
3. Anderson R., Roe M. A5. [Електронний ресурс] : http://jya.com/crack-a5.htm.
4. Komninos N., Honary B., Darnell M. An efficient stream cipher Alpha1 for mobile and wireless devices // Proceedings of the 8-th IMA International Conference on Cryptography and Coding. 2001. P. 294–300.
5. Simpson L.R. LILI Keystream Generator / L.R. Simpson, E. Dawson, J.D. Golić, W.L. Millan // Selected Are-as in Cryptography. SAC 2000. Lecture Notes in Computer Science, vol. 2012. Springer, Berlin, Heidelberg. P. 248–261.
6. Sadkhan S.B. A proposed Development of Clock Control Stream Cipher based on Suitable Attack // 2020 1st. Information Technology To Enhance e-learning and Other Application. IT-ELA, 2020, P. 165–170. doi: 10.1109/IT-ELA50150.2020.9253074.
7. Xu Y., Hao Y., Wang M. Revisit two memoryless state-recovery cryptanalysis methods on A5/1 // http://eprint.iacr.org /2023/1557.
8. Meneses A., van Oorschot P., Vanderstone S. Handbook of applied cryptography. CRC Press, 1997.
9. Kholosha A.A. Clock-controlled shift registers for key-stream generation // http://eprint.iacr.org /2001/061.
10. Gollman D., Chambers W.G. Clock-controlled shift registers: a review // IEEE J. on Selected Areas in Communication. 1989. V. 7. № 4. P. 525–533.
11. Golić J., O'Connor L. Embedding and probabilistic correlation attacks on clock-controlled shift registers // Advances in Cryptology – EUROCRYPT'94, Proceedings. Springer Verlag. 1995. P. 230 243.
12. Golić J., Petrovic M.V. A generalized correlation attacks with a probabilistic constrained edit distance // Advances in Cryptology – EUROCRYPT'92, Proceedings. Springer Verlag. 1992. P. 472–476.
13. Johansson T. Redused complexity correlation attacks on two clock-controlled generators // ASIACRYPT'98, Proceedings. Springer Verlag. 1998. P. 342–356.
14. Mikhailov G.V., Chistyakov V.P. On the problems of finite automatons theory related to the number of preimages of the output sequences // Review of Applied and Industrial Mathematics. 1994. Vol. 1, Iss. 1. P. 108–117.
15. Ekdahl P., Johansson T. Another attack on A5/1 // IEEE Trans. on Inform. Theory. 2003. Vol. 49. P. 1–7.
16. Ekdahl P. On LFSR-based stream cipher: analysis and design. Ph. D. Th., 2003.
17. Коваленко І.М., Гнеденко Б.В. Теорія ймовірностей. Київ : Вища шк., 1990. 328 с.
18. Feller W. An introduction to probability theory and its application. Willey. N.-Y., 1950. 420 p.

Надійшла до редколегії 17.09.2024

Відомості про авторів:

Олексійчук Антон Миколайович – доктор технічних наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", професор спеціальної кафедри № 1; Україна; e-mail: alex-dtn@ukr.net

Самойлов Ігор Володимирович – кандидат технічних наук, доцент, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", доцент спеціальної кафедри № 1; Україна; e-mail: samoilov1966igor@gmail.com