CRYPTOLOGY

DOI 10.20535/2411-1031.2024.12.1.306256
УДК 004.056

АЛЕКСАНДРА МАТІЙКО,
АНТОН ОЛЕКСІЙЧУК

ФІЛЬТРУВАЛЬНІ ГЕНЕРАТОРИ ГАМИ ЗІ ЗМІННИМИ ФУНКЦІЯМИ ПЕРЕХОДІВ НАД СКІНЧЕННИМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Фільтрувальні генератори гами є традиційною основою для створення синхронних потокових шифрів. Вони будуються за допомогою лінійних регістрів зсуву (як правило, над полем з двох елементів) та нелінійних функцій ускладнення, до яких висувається низка вимог з погляду стійкості генераторів відносно відомих атак. Інтенсивні дослідження фільтрувальних генераторів гами протягом останніх десятиліть показують, що задовольнити зазначені вимоги, не погіршуючи продуктивність генераторів, виявляється дуже складною задачею. Попри велику кількість публікацій, присвячених побудові функцій ускладнення з відомими “гарними криптографічними властивостями”, застосування таких функцій на практиці часто-густо стає неприйнятим внаслідок громіздкості їхніх конструкцій, що уповільнює функціонування відповідних генераторів, особливо при програмній реалізації.

У статті пропонується спосіб подолання відзначених труднощів шляхом застосування додаткового секретного параметра, що визначає вигляд функції переходів генератора. Така модифікація надає змогу підвищити стійкість генератора (в порівнянні з традиційними фільтрувальними генераторами гами) відносно відомих атак, не збільшуючи довжину його початкового стану. Зокрема, розглянуто конкретний варіант побудови генератора з функцією ускладнення, яка визначається за допомогою підстановок, що використовуються в алгоритмі шифрування “Калина”. Отримано нижню оцінку періодів вихідних послідовностей запропонованих генераторів. Проведено також дослідження їхньої стійкості відносно відомих атак, зокрема, атаки балансування типу Беббіджа-Голіча; атаки, пов’язаної з малою кількістю доданків у поліноміальному представленні функції ускладнення (що негативно відбивається на значенні еквівалентної лінійної складності вихідних послідовностей генератора); природної кореляційної атаки, пов’язаної зі специфікою запропонованої схеми побудови генератора; алгебраїчних атак типу Куртуа-Майєра. На завершенні статі зазначено, як вибирати компоненти запропонованих генераторів гами для забезпечення їхньої стійкості на заздалегідь визначеному рівні.

Ключові слова: криптографічний захист інформації, потоковий шифр, фільтрувальний генератор гами, функція переходів, алгебраїчна атака, статистична атака, обґрунтування стійкості.

Постановка проблеми. Фільтрувальний генератор гами з примітивним поліномом зворотного зв’язку $f(x)$ степеня n над полем $\mathbf{GF}(2)$ та функцією ускладнення $G:\{0,1\}^n \to \{0,1\}$ визначається як автономний автомат з множиною станів $\{0,1\}^n$, що функціонує за законом $\gamma_i = G(x_0 S^i)$, $i = 0, 1, \ldots$, де γ_i – знак вихідної послідовності генератора (або знак гами) в i-му такті, x_0 – початковий стан генератора, S – супровідна матриця полінома $f(x)$ (див., наприклад, [1]). Стійкість генератора відносно відомих атак визначається властивостями функції G. Відомо чимало різноманітних вимог до цієї функції, які в сукупності накладають на неї жорсткі обмеження, що ускладнює побудову або реалізацію

таких функцій (див. монографії [2], [3] та наведені у них посилання). Як наслідок, постає задача створення модифікованих фільтрувальних генераторів, які здатні забезпечити ту ж саму стійкість відносно відомих атак за менш обмежувальних вимог до їхній функцій ускладнення, що, у свою чергу, надасть змогу будувати одночасно стійки та практичні фільтрувальні генератори гами.

Мета статті полягає в тому, щоб запропонувати один з можливих варіантів вирішення цієї задачі.

Аналіз останніх досліджень і публікацій. Фільтрувальні генератори гами інтенсивно вивчаються протягом багатьох десятиліть і утворюють основу для побудови синхронних потокових шифрів. На сьогодні відомо чимало атак, які накладають жорсткі обмеження на функції ускладнення цих генераторів (див., наприклад, [1]–[4]). Зокрема, для забезпечення належної стійкості функція ускладнення повинна: бути зрівноваженою; мати достатньо велику алгебраїчну імунність (зокрема, достатньо великий степінь); мати велику нелінійність (бути віддаленою від афінних функцій); мати тривіальну лінійну структуру. Окрім того, вона не повинна мати "достатньо простого" представлення у вигляді полінома від однієї змінної над розширенням поля $\mathbf{GF}(2)$ (так званого трейс-представлення) [4]. Перелік подібних вимог постійно поповнюється, що приводить до різноманітних методів побудови булевих функцій з "гарними криптографічними властивостями". Список публікацій за цією тематикою нараховує десятки найменувань (див., наприклад, бібліографію в [3], [4]).

Попри різноманіття методів побудови функцій ускладнення з потрібними властивостями, більшість з них призводить до надто громіздких (або недостатньо прозорих) конструкцій, що є складними для реалізації (або виявляються слабкими з появою нових атак). Відзначимо роботу [5], де показано, як можна підвищити стійкість фільтрувального генератора до алгебраїчних атак, не змінюючи довжину його початкового стану або функцію ускладнення.

Нижче пропонується схожа конструкція генераторів гами, яка, поряд з тим, має більш простий аналітичний опис.

Виклад основного матеріалу дослідження.

1. Означення генератора гами. *Вхідними даними* для побудови генератора є такі об'єкти:

1) примітивний поліном $f(x)$ степеня n над полем $\mathbf{GF}(2)$, який визначає поле $F = \mathbf{GF}(2)[x]/(f(x))$ (надалі елементи цього поля ототожнюються з наборами їхніх координат у поліноміальному базисі $1, x, ..., x^{n-1}$);

2) підстановка $\Phi : F \to F$ така, що $\Phi(0) = 0$;

3) ненульовий вектор c довжини n над полем F.

Алгоритм генерації гами має такий вигляд:

1) згенерувати (таємне) випадкове рівноймовірне число $i_0 \in \overline{0,2^n - 1}$;

2) згенерувати (таємне) випадкове рівноймовірне число $j_0 \in \overline{0,2^n - 1}$, що є взаємно простим з $2^n - 1$:

3) обчислити в полі F елементи $\alpha = x^{i_0} \bmod f(x)$, $\theta = x^{j_0} \bmod f(x)$;

4) обчислити знаки гами, вважаючи

$$\gamma_i = c\Phi(\alpha\theta^i), \ i = 0, 1, ... \tag{1}$$

Зауважимо, що у формулі (1) $\alpha\theta^i$ позначає добуток зазначених елементів у полі F, а $c\Phi(\alpha\theta^i)$ – скалярний добуток над полем $\mathbf{GF}(2)$ вектора c на вектор, що складається з координат (у поліноміальному базисі) значення підстановки Φ у точці $\alpha\theta^i$.

Таким чином, для знаходження i-го знаку вихідної послідовності генератора треба обчислити елемент $\alpha\theta^i = x^{i_0+ij_0} \bmod f(x)$ поля F, застосувати до нього підстановку Φ та помножити скалярно її значення на вектор c.

Початковий стан генератора визначається парою чисел (i_0, j_0), які генеруються на кроках 1), 2) наведеного алгоритму. Кількість цих станів дорівнює $(2^n-1)\varphi(2^n-1) = (2^n-1)^2\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_u}\right)$, де φ позначає функцію Ойлера, $p_1,...,p_u$ – усі різні прості дільники числа 2^n-1.

Зауважимо також, що в наведеній конструкції генератора гами обидва параметри α і θ є секретними. Вважаючи $\theta = x \bmod f(x)$ (або $j_0 = 1$) отримаємо традиційний двійковий фільтрувальний генератор гами.

2. Нижня оцінка періоду вихідної послідовності генератора.

Твердження 1. Мінімальний період t послідовності (1) є не менше ніж 2^n-1.

Доведення. З рівності $\gamma_{i+t} = \gamma_i$, $i = 0,1,...$, та формули (1) випливає, що $c(\Phi(\theta^t\alpha\theta^i) - \Phi(\alpha\theta^i)) = 0$ для кожного невід'ємного цілого i. Оскільки θ є примітивним елементом поля F, то

$$c(\Phi(\theta^t x) - \Phi(x)) = 0,\ x \in F \tag{2}$$

Позначимо H підгрупу мультиплікативної групи поля F, породжену елементом θ^t, $l = \frac{2^n-1}{(2^n-1,\, t)}$ – її порядок (тут і далі $(2^n-1, t)$ позначає найбільший спільний дільник зазначених чисел). Позначимо також $L = \{y \in \mathbf{GF}(2)^n : cy = 0\}$. З формули (2) випливає, що для кожного $x \in F$ множина $\Phi(xH) = \{\Phi(x), \Phi(\theta^t x), ..., \Phi(\theta^{t(l-1)}x)\}$ міститься у деякому суміжному класі векторного простору $\mathbf{GF}(2)^n$ за підпростором L і, оскільки Φ є підстановкою, а $\Phi(0) = 0$, то кожен такий ненульовий суміжний клас є об'єднанням множин зазначеного вигляду, а сам підпростір L є об'єднанням цих множин та одноелементної множини, яка складається з нульового вектора. Отже, існують елементи $x_1,...,x_s \in F$ такі, що $L = \{0\} \cup \Phi(x_1H) \cup \cdots \cup \Phi(x_sH)$, де множини в об'єднанні попарно не перетинаються.

З останньої рівності випливає, що $|L| = 2^{n-1} = 1 + s|H| = 1 + sl$, тобто $sl = 2^{n-1}-1$ і l ділить $2^{n-1}-1$. Але $l = \frac{2^n-1}{(2^n-1,\, t)}$ ділить також число 2^n-1 а, отже, й число $2^n - 1 - 2(2^{n-1}-1) = 1$. Таким чином, $(2^n-1, t) = 2^n-1$, отже, t ділиться на число 2^n-1.

Твердження доведено.

3. Оцінка стійкості генератора відносно атаки Беббіджа-Голіча. Зазначена атака [6], [7] складається з двох етапів, на першому з яких криптоаналітик генерує деяку кількість M попарно різних початкових станів генератора, за якими обчислює відрізки вихідних послідовностей. Ці відрізки (поряд з відповідними початковими станами) зберігаються у

заздалегідь сформованій таблиці. На другому етапі атаки криптоаналітик отримує доступ до D різних відрізків гами, вироблених генератором при різних невідомих початкових станах. У випадку знаходження хоча б одного з цих відрізків у таблиці криптоаналітик знаходить відповідний початковий стан генератора, що є метою атаки.

Якщо число початкових станів генератора дорівнює N, то, за умови $MD \geq CN$ (де $C \geq 1$) та деяких природних ймовірнісних припущень, атака завершується успішно із ймовірністю не менше ніж $1-e^{-C}$ (див., наприклад, [1]). Зокрема, вважаючи $D = N^{1/2}$, $M = CN^{1/2}$, отримаємо, що трудомісткість атаки становить $T = O(N^{1/2})$.

Таким чином, для забезпечення стійкості генератора відносно розглянутої атаки на рівні 2^{λ} достатньо виконання умови $N \geq 2^{2\lambda}$, де $N = (2^n - 1)^2\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_u}\right)$, $p_1, ..., p_u$ – усі різні прості дільники числа $2^n - 1$.

4. Обмеження щодо вибору підстановки Ф, виходячи з оцінки еквівалентної лінійної складності гами. Нагадаємо, що еквівалентна лінійна складність будь-якої лінійної рекурентної послідовності над полем визначається як степінь мінімального полінома цієї послідовності, тобто полінома найменшого степеня над заданим полем, який анулює цю послідовність (див., наприклад, [2]).

Довільна підстановка Ф над полем F однозначно задається за допомогою полінома:

$$\Phi(x) = \sum_{j=0}^{d} f_j x^j, \ x \in F \tag{3}$$

де $f_j \in F$, $j \in \overline{0,d}$, $d \leq 2^n - 1$.

Твердження 2. За умови (3) еквівалентна лінійна складність послідовності (1) не перевищує nr, де r – число ненульових доданків у виразі полінома (3).

Доведення. З формул (1), (3) випливає, що

$$\gamma_i = c\Phi(\alpha\theta^i) = c\left(\sum_{j=0}^{d} f_j(\alpha\theta^i)^j\right) = \sum_{j=0}^{d} c(f_j\alpha^j\theta^{ji}), \ i = 0, 1, ... \tag{4}$$

Для кожного $j \in \overline{0,d}$ такого, що $f_j \neq 0$, позначимо $\gamma_{i,j} = c(f_j\alpha^j\theta^{ji})$, $i = 0, 1, ...$ Помітимо, що елементи $1, \theta^j, ..., \theta^{j(n-1)}, \theta^{jn}$ поля F є лінійно залежними над полем $\mathbf{GF}(2)$, звідки випливає, що існує натуральне число $k \leq n$ таке, що елемент θ^{jk} є лінійною комбінацією елементів $1, \theta^j, ..., \theta^{j(k-1)}$ з коефіцієнтами, які належать цьому полю. Але тоді для кожного $i = 0, 1, ...$ елемент $\gamma_{i+k,j}$ є лінійною комбінацією елементів $\gamma_{i,j}, \gamma_{i+1,j}, ..., \gamma_{i+k-1,j}$ з такими самими коефіцієнтами.

Отже, послідовність $(\gamma_{i,j} : i = 0, 1, ...)$ анулюється поліномом степеня $k \leq n$ над полем $\mathbf{GF}(2)$, і на підставі формули (4) послідовність $(\gamma_i : i = 0, 1, ...)$ анулюється добутком зазначених поліномів за всіма $j \in \overline{0,d}$ такими, що $f_j \neq 0$.

Таким чином, еквівалентна лінійна складність послідовності (4) не перевищує nr, що й треба було довести.

Отримане твердження показує, що при побудові генератора гами не можна вибирати підстановку Ф, яка задається поліномом над полем F з невеликою кількістю доданків. Зокрема, не можна вибирати в ролі Ф будь-яку степеневу підстановку, навіть за умови, що

вона має певні гарні криптографічні властивості, наприклад, є майже досконало нелінійною або майже бент-підстановкою (див., наприклад, [8]).

Виходячи з цього, пропонується вибирати підстановки, які будуються за допомогою нелінійних вузлів заміни, що використовуються в сучасних блокових шифрах.

5. Спосіб побудови підстановки Φ**.** Для будь-якого натурального m позначимо V_m множину двійкових векторів довжини m. Для будь-якої підстановки $s: V_m \to V_m$ та довільних векторів $b, c \in V_m$ позначимо

$$l_s(b,c) = \left| \sum_{x \in V_m} (-1)^{cs(x) \oplus bx} \right|, \tag{5}$$

де $cs(x)$ та bx позначають булеві скалярні добутки зазначених двійкових векторів.

Зауважимо, що параметр (5) співпадає з модулем коефіцієнта Уолша-Адамара функції cs в точці b.

Припустимо, що $n = pt$, де p, t – натуральні числа, $p, t \geq 2$. Зафіксуємо підстановки (s-блоки) $s_1, ..., s_p$ на множині V_t та визначимо підстановку $s: V_n \to V_n$, вважаючи $s(x) = (s_1(x_1), ..., s_p(x_p))$, $x = (x_1, ..., x_p)$, $x_j \in V_t$, $j \in \overline{1, p}$. Нарешті, задамо підстановку Φ за формулою

$$\Phi(x) = s(x) \oplus s(0), \; x \in V_n \tag{6}$$

Зауважимо, що $\Phi(0) = 0$.

Твердження 3. За умови (6) для довільного вектора $c = (c_1, ..., c_p)$ такого, що $c_j \in V_t \setminus \{0\}$, $j \in \overline{1, p}$, нелінійність булевої функції $c\Phi$ дорівнює

$$N_{c\Phi} = 2^{n-1} - 1/2 \cdot \prod_{j=1}^{p} \max_{b_j \in V_t \setminus \{0\}} l_{s_j}(b_j, c_j), \tag{7}$$

Доведення. Справедливість рівності (7) випливає безпосередньо з означення нелінійності: $N_{c\Phi} = 2^{n-1} - 1/2 \cdot \max\limits_{b \in V_n} \left| \sum\limits_{x \in V_n} (-1)^{c\Phi(x) \oplus bx} \right|$, формул (5), (6) та умови $c_j \in V_t \setminus \{0\}$, $j \in \overline{1, p}$.

Наведений результат надає змогу запропонувати такий алгоритм вибору вектора c для визначення функції $c\Phi$, що має найбільшу можливу (у визначеному класі функцій) нелінійність

Алгоритм 1.

Вхідні дані: натуральні числа $p, t \geq 2$ такі, що $n = pt$; підстановки $s_1, ..., s_p$ на множині V_t.

1. Для всіх $j \in \overline{1, p}$, $c_j \in V_t \setminus \{0\}$:

– обчисли значення

$$l_{s_j}(b_j, c_j) = \left| \sum_{x \in V_t} (-1)^{c_j s_j(x_j) \oplus b_j x_j} \right|, \; b_j \in V_t \tag{8}$$

використовуючи алгоритм швидкого перетворення Адамара (див., наприклад, [1]);

– визначити вектор $b_j^* \in V_t$, на якому досягається максимуму значень (8) за всіма $b_j \in V_t$;

2. Для кожного $j \in \overline{1, p}$ визначити вектор $c'_j \in V_t \setminus \{0\}$ такий, що

$$l_{s_j}(b_j^*, c'_j) = \min_{c_j \in V_t \setminus \{0\}} l_{s_j}(b_j^*, c_j).$$

Результат: вектор $c = (c'_1, ..., c'_p)$.

Таким чином, для побудови генератора гами пропонується вибирати підстановку Φ у вигляді (6), а вектор c – за допомогою алгоритму 1. Це надає змогу оптимізувати стійкість генератора відносно кореляційної атаки, яка розглядається нижче.

6. Оцінка стійкості генератора відносно кореляційної атаки, спрямованої на відновлення мінімального полінома елемента θ. Нагадаємо, що секретними параметрами, від яких залежить вихідна послідовність генератора, є елементи α і θ поля F. Мінімальний поліном над полем з двох елементів (примітивного) елемента θ має вигляд $m(z) = m_0 \oplus m_1 z \oplus \cdots \oplus m_{n-1} z^{n-1} \oplus z^n$, де $m_0 = 1$. Цей поліном визначає рекурентний закон, за яким формуються члени послідовності $(\alpha\theta^i : i = 0, 1, ...)$:

$$\alpha\theta^{i+n} = m_0 \alpha\theta^i \oplus m_1 \alpha\theta^{i+1} \oplus \cdots \oplus m_{n-1} \alpha\theta^{i+n-1}, \; i = 0, 1, ... \tag{9}$$

Для отримання апостеріорної інформації про невідомий елемент θ криптоаналітик може спробувати знайти поліном $m(z)$ за вихідною послідовністю генератора, використовуючи кореляційну атаку, яка полягає у виборі лінійного наближення $l(x) = bx, \; x \in F$ функції $c\Phi$ та розв'язанні системи лінійних рівнянь зі спотвореними правими частинами.

Рівняння будуються таким чином. Для будь-якого $i = 0, 1, ...$ позначимо $\xi_i = \gamma_i \oplus b(\alpha\theta^i)$, де γ_i – знак вихідної послідовності генератора, що визначається за формулою (1). Використовуючи формулу (9), отримаємо рівності

$$\gamma_{i+n} = b(\alpha\theta^{i+n}) \oplus \xi_{i+n} = m_0 b(\alpha\theta^i) \oplus m_1 b(\alpha\theta^{i+1}) \oplus \cdots \oplus m_{n-1} b(\alpha\theta^{i+n-1}) \oplus \xi_{i+n} =$$
$$= m_0 \gamma_i \oplus m_1 \gamma_{i+1} \oplus \cdots \oplus m_{n-1} \gamma_{i+n-1} \oplus$$
$$\oplus m_0 \xi_i \oplus m_1 \xi_{i+1} \oplus \cdots \oplus m_{n-1} \xi_{i+n-1} \oplus \xi_{i+n}, \; i = 0, 1, ...,$$

які (з урахуванням умови $m_0 = 1$) можна записати в такому вигляді:

$$m_1 \gamma_{i+1} \oplus \cdots \oplus m_{n-1} \gamma_{i+n-1} \oplus \eta_i = \gamma_{i+n} \oplus \gamma_i, \tag{10}$$

$$\eta_i = \xi_i \oplus m_1 \xi_{i+1} \oplus \cdots \oplus m_{n-1} \xi_{i+n-1} \oplus \xi_{i+n}, \; i = 0, 1, ... \tag{11}$$

Припустимо, що $\xi_0, \xi_1, ...$ є незалежними випадковими величинами, розподіленими за законом $\mathbf{P}(\xi_i = 0) = 1 - \mathbf{P}(\xi_i = 1) = \mathbf{P}(c\Phi(X) = bX)$, де X – випадковий рівноймовірний двійковий вектор довжини n. Тоді співвідношення (10), (11) утворюють систему лінійних рівнянь зі спотвореними правими частинами відносно коефіцієнтів невідомого полінома $m(z)$. Вибираючи з цієї системи рівняння з номерами $i_1, i_2, ...$ такими, що $i_{j+1} - i_j > n$ для кожного $j = 0, 1, ...,$ отримаємо кінцеву систему рівнянь із незалежними спотвореннями у правих частинах.

Кількість рівнянь у побудованій системі, необхідних для її розв'язання із заданою (високою) ймовірністю, характеризує стійкість генератора відносно наведеної кореляційної атаки. (Зазначена кількість є нижньою межею часової складності будь-якого алгоритму

розв'язання побудованої системи рівнянь; при цьому генератор є обґрунтовано стійким, якщо кількість рівнянь у системі є не менше визначеного рівня 2^{λ}).

Твердження 4. Нехай m позначає найменше число рівнянь у побудованій системі, для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$. Тоді

$$m \geq \frac{n(1-\delta) - h(\delta)}{(1 - 2^{-(n-1)} N_{c\Phi})^6} \ln 2, \tag{12}$$

де $N_{c\Phi}$ – нелінійність функції $c\Phi$, $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$.

Доведення. Скористаємося теоремою 2 у статті [9], згідно з якою за умов (10), (11) (та незалежності спотворень у правих частинах рівнянь побудованої системи) має місце оцінка

$$m \geq \frac{n(1-\delta) - h(\delta)}{(1 - 2\mathbf{P}(\eta_i = 0))^2} \ln 2.$$

Далі, помітимо, що на підставі (11) та незалежності випадкових величин $\xi_0, \xi_1, \ldots$ виконується рівність $(1-\mathbf{P}(\eta_i = 0))^2 = (1-\mathbf{P}(\xi_i = 0))^2 (1-\mathbf{P}(\xi_{i+n} = 0))^2 \prod\limits_{j \in \overline{1, n-1}: m_j = 1} (1-\mathbf{P}(\xi_{i+j} = 0))^2$, з якої на підставі співвідношень $\mathbf{P}(\xi_{i+j} = 0) = \mathbf{P}(c\Phi(X) = bX)$, $j = 0, 1, \ldots$, $|\{j \in \overline{1, n-1}: m_j = 1\}| \geq 1$ випливає, що $(1-\mathbf{P}(\eta_i = 0))^2 \leq (1 - 2\mathbf{P}(c\Phi(X) = bX))^6$. Нарешті, згідно з означенням нелінійності функції $c\Phi$ маємо $|1 - 2\mathbf{P}(c\Phi(X) = bX)| \leq \max\limits_{b \in V_n} \left| 2^{-n} \sum\limits_{x \in V_n} (-1)^{c\Phi(x) \oplus bx} \right| = 1 - 2^{-(n-1)} N_{c\Phi}$. З наведених співвідношень випливає оцінка (12).

Таким чином, на підставі тверджень 3 і 4, можна оцінити часову складність розглянутої кореляційної атаки на генератор гами величиною порядку $l^{-6} p$, де l дорівнює максимуму значень $2^{-t} l_{s_j}(b_j^*, c_j')$ за всіма $j \in \overline{1, p}$ (див. алгоритм 1).

Як приклад, розглянемо генератор, побудований за визначеною вище схемою для $p = 64$, $t = 8$ ($n = 512$), вважаючи, що підстановки $s_1, \ldots, s_p$ вибираються серед s-блоків, які використовуються в алгоритмі шифрування "Калина" [10].

Відомо [11], що $\max\limits_{j \in \overline{1, p}} \{2^{-t} l_{s_j}(b_j^*, c_j')\} \leq 3 \cdot 2^{-4} < 2^{-2}$, звідки випливає, що складність кореляційної атаки на генератора становить не менше ніж $(2^{-2})^{6 \cdot 64} = 2^{768}$.

7. Оцінка стійкості генератора відносно алгебраїчних атак. Продовжимо дослідження властивостей генератора гами за умови, що підстановка Φ визначається за формулою (6), а вектор c – за допомогою алгоритму 1.

Алгебраїчні атаки мають на меті відновлення початкового стану цього генератора (тобто елементів α і θ поля F) за його вихідною послідовністю шляхом розв'язання системи рівнянь (1). Загальна схема побудови таких атак полягає у знаходженні систем, що складаються з рівнянь якомога меншого степеня, які є наслідками системи (1), та у розв'язанні отриманих систем-наслідків за допомогою відомих методів [2], [12]–[15].

Для того, щоб описати вигляд шуканих рівнянь, доведемо два допоміжних твердження.

Лема 1. Нехай $f(x) = x^n \oplus c_{n-1} x^{n-1} \oplus \cdots \oplus c_0$ – примітивний поліном над полем з двох елементів, що використовується для означення поля F, з якого вибираються елементи α і

θ. Позначимо $u=(u_0,u_1,...,u_{n-1})$ та $v=(v_0,v_1,...,v_{n-1})$ відповідно вектори координат цих елементів у поліноміальному базисі поля F. Позначимо також

$$S=\begin{pmatrix} 0\,1\,0\,...\,0 \\ 0\,0\,1\,...\,0 \\ ...\ ...\ ... \\ 0\,0\,0\,...\,1 \\ c_0\,c_1\,...\,c_{n-1} \end{pmatrix}$$

супровідну матрицю полінома $f(x)$. Тоді для будь-якого $i=0,1,...$ вектор коефіцієнтів елемента $\alpha\theta^i$ дорівнює добутку вектор-рядка u на матрицю

$$v(S)=v_0S^0\oplus v_1S^1\oplus\cdots\oplus v_{n-1}S^{n-1}. \tag{13}$$

Доведення. Для будь-якого $a\in\mathbf{GF}(2^n)$ позначимо $\hat{a}=(a_0,a_1,...,a_{n-1})$ вектор-рядок координат елемента a в поліноміальному базисі поля F. Позначимо також $a(S)=a_0S^0\oplus a_1S^1\oplus\cdots\oplus a_{n-1}S^{n-1}$.

Для доведення леми достатньо переконатися, що вектор координат добутку будь-яких елементів $a,b\in\mathbf{GF}(2^n)$ дорівнює $\hat{a}b(S)$. Доведемо це.

Позначимо e_i вектор координат базисного елемента x^i поля F, $i\in\overline{0,n-1}$. Помітимо, що

$$e_0a(S)=\hat{a}. \tag{14}$$

Дійсно, використовуючи індукцію за i, нескладно перевірити, що $e_0S^i=e_i$, $i\in\overline{0,n-1}$, і, отже,

$$e_0a(S)=\sum_{i=0}^{n-1}a_ie_0S^i=\sum_{i=0}^{n-1}a_ie_i=\hat{a}.$$

Далі, оскільки $f(x)$ є мінімальним поліномом матриці S, то відображення $a\mapsto a(S)$ є ізоморфізмом поля F в поле, що складається з усіх матриць вигляду $b(S)$, де $b\in F$. При цьому ізоморфізмі елементу ab відповідає матриця $a(S)b(S)$ і на підставі формули (14), послідовно застосованої до елементів ab и a, вектор координат елемента ab дорівнює $e_0a(S)\,b(S)=\hat{a}\,b(S)$.

Лему доведено.

Друге допоміжне твердження пов'язане з поняттям алгебраїчної імунності булевої функції $f:V_n\to\{0,1\}$, яке визначається як найменший степінь усіх ненульових рівнянь вигляду $F(x)=0$, де $F:V_n\to\{0,1\}$, які є наслідками хоча б одного рівняння $f(x)=0$, $f(x)=1$ (див., наприклад, [1]).

Лема 2. Нехай підстановка Φ визначається за формулою (6), а вектор $c=(c'_1,...,c'_p)$ – за допомогою алгоритму 1. Тоді алгебраїчна імунність функції $c\Phi$ є не менше ніж максимум алгебраїчних імунностей функцій c'_js_j за всіма $j\in\overline{1,p}$.

Доведення. Позначимо $\mathrm{AI}(f)$ алгебраїчну імунність довільної булевої функції f. Для доведення леми достатньо показати, що за умови $f(x,y)=g(x)\oplus h(y)$, $x\in V_n$, $y\in V_m$, справедлива нерівність $\mathrm{AI}(f)\ge\max\{\mathrm{AI}(g),\mathrm{AI}(h)\}$.

Дійсно, нехай $F(x,y)=0$ є наслідком рівняння $f(x,y)=\gamma$, де $\gamma\in\{0,1\}$, $F:V_{n+m}\to\{0,1\}$ і $\deg F=\mathrm{AI}(f)$. Зафіксуємо вектори $x_0\in V_n$, $y_0\in V_m$ такі, що $F(x_0,y_0)=1$. Помітимо, що рівняння $F(x,y_0)=0$ є наслідком рівняння $g(x)=\gamma\oplus h(y_0)$ і, отже, степінь (ненульової) булевої функції $F(x,y_0)$, $x\in V_n$ є не менше ніж $\mathrm{AI}(g)$. Але зазначений степінь не перевищує $\deg F$, звідки випливає нерівність $\mathrm{AI}(f)\ge\mathrm{AI}(g)$. Аналогічно отримаємо, що $\mathrm{AI}(f)\ge\mathrm{AI}(h)$.

Лему доведено.

Повернемося до системи рівнянь (1) та помітимо, що за допомогою леми 1 її можна перетворити на систему булевих рівнянь від $2n$ невідомих $u_0,u_1,...,u_{n-1}$ та $v_0,v_1,...,v_{n-1}$, які є координатами шуканих елементів α і θ відповідно. Дійсно, i-е рівняння такої системи має вигляд

$$c\Phi((u_0,u_1,...,u_{n-1})v(S)^i)=\gamma_i,\ i=0,1,...,\qquad(15)$$

де матриця $v(S)$ визначається за формулою (13).

Помітимо далі, що $v(S)^i=v_0S^0\oplus v_1S^i\oplus\cdots\oplus v_{n-1}S^{i(n-1)}\oplus w_i(S)$, де $w_i(S)$ є сумою всіх добутків $v_{k_1}v_{k_2}\cdots v_{k_i}S^{k_1+k_2+\cdots+k_i}$ таких, що серед чисел $k_1,k_2,...,k_i\in\overline{0,n-1}$ є принаймні два різних. Звідси випливає, що кожен ненульовий елемент матриці $v(S)^i$ є поліномом від змінних $v_0,v_1,...,v_{n-1}$, степінь якого є не менше за 1 (причому, може дорівнювати 1, наприклад, якщо i є степенем двійки). Отже, координати вектора $(u_0,u_1,...,u_{n-1})v(S)^i$ під знаком функції $c\Phi$ у правій частині рівняння (15) є поліномами степеня не менше ніж 2 від змінних $u_0,u_1,...,u_{n-1}$, $v_0,v_1,...,v_{n-1}$.

Для зменшення степенів рівнянь у системі (15) розглянемо довільну функцію F від зазначених змінних таку, що $\deg F=\mathrm{AI}(c\Phi)$, а рівняння $F(u,v)=0$ є наслідком одного з рівнянь $c\Phi(u,v)=0$, $c\Phi(u,v)=1$. Використовуючи F як описано в [12], отримаємо систему рівнянь-наслідків системи (15), степені яких обмежені знизу числом $2\mathrm{AI}(c\Phi)$, яке, у свою чергу (згідно з лемою 2), є не менше ніж максимум значень $2\mathrm{AI}(c'_js_j)$ за всіма $j\in\overline{1,p}$. Отримана інформація надає змогу оцінити знизу складність розв'язання системи рівнянь (15) за допомогою відомих методів [2], [12]–[15].

Як приклад, розглянемо випадок, коли $p=64$, $t=8$ ($n=512$), а підстановки $s_1,...,s_p$ вибираються серед s-блоків алгоритму шифрування "Калина". На підставі [16] для кожного $c_j\in V_8\setminus\{0\}$ має місце рівність $\mathrm{AI}(c_js_j)=3$. Отже, для знаходження значень $u_0,u_1,...,u_{n-1}$, $v_0,v_1,...,v_{n-1}$ треба розв'язати систему рівнянь не менше ніж 6-го степеня від $2n=2^{10}$ невідомих. Складність розв'язання такої системи методом введення нових змінних є величиною порядку $\left(\frac{(2n)^6}{6!}\right)^3>2^{150}$ за умови, що кількість рівнянь у системі (тобто кількість доступних знаків гами) є не менше ніж $\frac{(2n)^6}{6!}$. Така ж сама за порядком величини кількість рівнянь потрібна для застосовності інших відомих методів розв'язання системи вигляду (15) [2], [13]–[15].

Таким чином, обмежуючи число знаків гами, які виробляє генератор при довільному фіксованому початковому стані, величиною 2^{50}, унеможливимо проведення на цей генератор відомих алгебраїчних атак, ефективніших за повний перебір.

Висновки

1. Для практичних застосувань пропонується використовувати генератор гами, описаний в п. 1, з такими параметрами (компонентами):

1) $n = 512$;

2) підстановка Ф визначається за формулою (6), де $p = 64$, $t = 8$, а підстановки $s_1, ..., s_p$ вибираються серед s-блоків алгоритму шифрування “Калина”;

3) вектор c вибирається за допомогою алгоритму 1.

Кількість знаків гами, які виробляються за будь-яким фіксованим початковим станом генератора, слід обмежити величиною 2^{50}.

2. Число початкових станів генератора (яке визначає його стійкість відносно повного перебору) дорівнює $N = (2^{512} - 1)\varphi(2^{512} - 1)$, де φ – функція Ойлера (значення $\varphi(2^{512} - 1)$ можна обчислити, використовуючи дані про розклади на прості співмножники чисел Ферма $F_0, F_1, ..., F_8$ [17], с. 29).

3. Період вихідної послідовності генератора є не менше за $2^{512} - 1$ для будь-якого початкового стану.

4. Стійкість генератора відносно атаки Беббіджа-Голіча є величиною порядку $N^{1/2}$ (яка є не набагато менше за 2^{512}).

5. Стійкість генератора відносно відомих кореляційних атак становить 2^{768}, а його стійкість відносно відомих алгебраїчних атак є величиною порядку N.

6. Примітивний поліном $f(x)$, що визначає поле $F = \mathbf{GF}(2^{512})$, над яким будується генератор, слід вибирати, виходячи з умов ефективної реалізації арифметики цього поля. Вигляд полінома не впливає на стійкість генератора до сучасних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] 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: Лют. 20, 2024.

[2] T.W. Cusick, and P. Stanica, *Cryptographic Boolean Functions and Applications*. San Diego, California, USA: Academic Press is an imprint of Elsevier, 2009.

[3] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, LAGA, University of Paris 8, France, 2007.

[4] A. Canteaut, and Y. Rotella, “Attacks against Filter Generators Exploiting Monomial Mappings”, *Cryptology ePrint Archive, Paper 2016/389*. [Online]. Available: https://ia.cr/2016/384. Accessed on: Feb. 23, 2024.

[5] А.М. Олексійчук, та К.І. Воробей, “Фільтрувальні генератори гами з підвищеною стійкістю відносно алгебраїчних атак”, *Information Technology and Security,* vol. 11, iss. 2 (21), pp. 149-155, July–December 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.2.293748.

[6] S. Babbage, “A space/time tradeoff in exhaustive search attacks on stream ciphers”, in *IEE Conf. Pub. European Convention on Security and Detection*, Brighton, 1995, no. 408.

[7] J.Dj. Golić, “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.

[8] C. Carlet, *Vectorial Boolean Functions for Cryptography*, LAGA, University of Paris 8, France, 2006.

[9] А.М. Олексійчук, та М.В. Поремський, “Нижні межі інформаційної складності кореляційних атак на потокові шифри над полями порядку 2^r”, *Захист інформації,* т. 19, № 2, с. 126-131, 2017, doi: https://doi.org/10.18372/2410-7840.19.11435.

[10] R. Oliynykov et al., “A New Encryption Standard of Ukraine: The Kalyna Block Cipher”, *Cryptology ePrint Archive, Paper 2015/650*. [Online]. Available: https://ia.cr/2015/650. Accessed on: Mar. 4, 2024.

[11] А.Н. Алексейчук, Л.В. Ковальчук, А.С. Шевцов, та С.В. Яковлев, “О криптографических свойствах нового национального стандарта шифрования Украины”, *Кібернетика та системний аналіз,* т. 52, № 3, с. 16-32, 2016. Електронний ресурс]. Доступно: http://www.kibernetika.org/volumes/2016/numbers/03/articles/02/2.pdf. Дата звернення: Бер.12, 2024.

[12] N. Courtois, and W. Meier, “Algebraic attacks on stream ciphers with linear feedback”, in *Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 345-359, 2003, doi: https://doi.org/10.1007/3-540-39200-9_21.

[13] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, “Efficient algorithms for solving overdefined systems of multivariate polinomial equations”, *in Proc. Advanced in Cryptology – EUROCRYPT 2000,* Springer Verlag, pp. 392-407, 2000, doi: https://doi.org/10.1007/3-540-45539-6_27.

[14] N. Courtois, “Fast algebraic attacks on stream ciphers with linear feedback”, in *Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 177-194, 2003, doi: https://doi.org/10.1007/978-3-540-45146-4_11.

[15] L. Bettale, J.-C. Faugere, and L. Perret “Hybrid approach for solving multivariate systems over finite fields”, *Journal of Mathematical Cryptology,* vol. 3, pp. 177-196, 2009, doi: https://doi.org/10.1515/JMC.2009.009.

[16] Р.В. Олійников, І.Д. Горбенко, О.В. Казимиров, В.І. Руженцев та Ю.І. Горбенко, “Принципи побудови і основні властивості нового національного стандарту блокового шифрування України”, *Захист інформації*, т. 17, № 2, с. 142-157, 2015, doi: https://doi.org/10.18372/2410-7840.17.8789.

[17] R. Crandall, and C.Pomerance, *Prime numbers. A computational perspective*, USA: Springer, 2005.

Стаття надійшла до редакції 20.05.2024.

REFERENCES

[1] A.N. Alekseychuk, and O.V. 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: Feb. 20, 2024.

[2] T.W. Cusick, and P. Stanica, *Cryptographic Boolean Functions and Applications*. San Diego, California, USA: Academic Press is an imprint of Elsevier, 2009.

[3] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, LAGA, University of Paris 8, France, 2007.

[4] A. Canteaut, and Y. Rotella, "Attacks against Filter Generators Exploiting Monomial Mappings", *Cryptology ePrint Archive, Paper 2016/389*. [Online]. Available: https://ia.cr/2016/384. Accessed on: Feb. 23, 2024.

[5] A.N. Alekseychuk, and K.I. Vorobei, "Filter generators with increased resistance against algebraic attacks", *Information Technology and Security*, vol. 11, iss. 2 (21), pp. 149-155, July–December 2023, doi: https://doi.org/10.20535/2411-1031.2023.11.2.293748.

[6] S. Babbage, "A space/time tradeoff in exhaustive search attacks on stream ciphers in *IEE Conf. Pub. European Convention on Security and Detection*, Brighton, 1995, no. 408.

[7] J.Dj. Golić, "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.

[8] C. Carlet, *Vectorial Boolean Functions for Cryptography*, LAGA, University of Paris 8, France, 2006.

[9] A.N. Alekseychuk, and M.V. Poremskyi, "Lover bounds for the data complexity of correlation attacks on stream ciphers over fields of order 2^r", *Ukrainian Information Security Research Journal*, vol. 19, № 2, с. 126-131, 2017, doi: https://doi.org/10.18372/2410-7840.19.11435.

[10] R. Oliynykov et al., "A New Encryption Standard of Ukraine: The Kalyna Block Cipher", *Cryptology ePrint Archive, Paper 2015/650*. [Online]. Available: https://ia.cr/2015/650. Accessed on: Mar. 4, 2024.

[11] A.N. Alekseychuk, L.V. Kovalchuk, A.S. Shevtsov, and S.V. Yakovliev, "Cryptographic properties of the new national encryption standard of Ukraine", *Cybernetics and systems analysis*, vol. 52, № 3, с. 16-32, 2016. [Online]. Available: http://www.kibernetika.org/volumes/2016/numbers/03/articles/02/2.pdf. Accessed on: Mar. 12, 2024.

[12] N. Courtois, and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", *in Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 345-359, 2003, doi: https://doi.org/10.1007/3-540-39200-9_21.

[13] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polinomial equations", *in Proc. Advanced in Cryptology – EUROCRYPT 2000*, Springer Verlag, pp. 392-407, 2000, doi: https://doi.org/10.1007/3-540-45539-6_27.

[14] N. Courtois, "Fast algebraic attacks on stream ciphers with linear feedback", in *Proc. Advanced in Cryptology – EUROCRYPT 2003*, Springer Verlag, pp. 177-194, 2003, doi: https://doi.org/10.1007/978-3-540-45146-4_11.

[15] L. Bettale, J.-C. Faugere, and L. Perret "Hybrid approach for solving multivariate systems over finite fields", *Journal of Mathematical Cryptology*, vol. 3, pp. 177-196, 2009, doi: https://doi.org/10.1515/JMC.2009.009.

[16] P.V. Oliynykov, I.D. Gorbenko, O.V. Kazymyrov, V.I. Ruzhentsev та I.I. Gorbenko, "Design principles and main properties of the new Ukrainian national standard of block encryption", *Ukrainian Information Security Research Journal*, vol. 17, № 2, с. 142-157, 2015, doi: https://doi.org/10.18372/2410-7840.17.8789.

[17] R. Crandall, and C.Pomerance, *Prime numbers. A computational perspective*, USA: Springer, 2005.

ALEXANDRA MATIYKO,
ANTON ALEKSEYCHUK

FILTER GENERATORS WITH VARIABLE TRANSITION FUNCTIONS OVER FINITE FIELDS OF CHARACTERISTIC 2

Filter generators are a traditional basis for creating synchronous stream ciphers. They are built with the help of linear shift registers (usually over a field of two elements) and nonlinear complexity functions, which are subject to a number of requirements in terms of the generators security against known attacks. Intensive researches of filter generators during the last decades show that meeting these requirements without degrading the performance of the generators is a very difficult task. Despite a large number of publications devoted to the construction of complexity functions with known "good cryptographic properties", the usage of such functions in practice often becomes unacceptable due to the bulkiness of their constructions, which slows down the functioning of the corresponding generators, especially during software implementation.

The way to overcome the noted difficulties by using an additional secret parameter that determines the appearance of the generator transitions' function is proposed. Such a modification makes it possible to increase the security of generator (compared to traditional filter generators) against known attacks without increasing the length of its initial state. In particular, a specific version of a generator construction with a complexity function, which is determined with the help of substitutions used in the "Kalyna" encryption scheme, is considered. A lower estimate of the output sequences periods of the proposed generators was obtained. A research of their security to known attacks, in particular, Babbage-Golic balancing attack; an attack associated with a small number of terms in the polynomial representation of the complexity function (which negatively affects the value of the equivalent linear complexity of the output sequences of the generator); a natural correlation attack associated with the specifics of the proposed generator construction scheme; algebraic attacks of the Courtois-Mayer type were also conducted. At the end of the article, it is indicated how to choose the components of the proposed generators to ensure their security at a predetermined level.

Keywords: cryptographic protection of information, stream cipher, filter generator, transition function, algebraic attack, statistical attack, security proof.

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.