УДК 681.32

ПОТОКОВЕ ШИФРУВАННЯ НА ОСНОВІ ТЕОРІЇ ЛІНІЙНОЇ ПОСЛІДОВНІСНОЇ МАШИНИ

В. П. Семеренко, Ю.В. Степанишин, М.Л. Гаєвський

Вступ

Схеми захисту інформації на основі поточного шифрування [1] широко застосовуються в сучасній техніці завдяки високій швидкості роботи та простій апаратній і програмній реалізацій. Відомо також [2], що окремо взятий базовий елемент цих схем - регістр зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) - дуже уразливий до кореляційних атак зламу. Тому для підвищення криптостійкості в сучасних потокових шифрах використовують різні способи введення нелінійності. Однак поки що не створено закінченого теоретичного базису для побудови схем із нелінійним зворотним зв'язком. Більшість сучасних публікацій в сфері потокових шифрів [3],[4] присвячено лише аналізу слабких місць та розробці методів зламу відомих шифрів. Актуальною залишається задача математичного обгрунтування криптографічних схем на основі регістрів зсуву як з лінійним, так із нелінійним зворотними зв'язками, і розробці нових программно-апаратних засобів потокового шифрування.

Мета роботи

Ця робота присвячена аналізу схем потокового шифрування і дешифрування на основі теорії лінійної послідовнісної машини та розробці нових криптографічних методів захисту інформації.

Постановка задачі потокового шифрування з позицій теорії ЛПМ

Переважна більшість відомих схем потокового шифрування базується на використанні регістрів зсуву дуже простої структури, що дає можливість використовувати для їх аналізу достатньо простий математичний апарат, зокрема, алгебраїчну теорію багаточленів над полем Галуа GF(2). Однак РЗЛЗЗ є лише окремим випадком лінійної послідовнісної схеми, або, як її ще називають, лінійної послідовнісної машини (ЛПМ) [5],[6]. Для представлення принципу роботи ЛПМ можна використати теорію автоматів, теорію імпульсних систем і загальну теорію керування. Використовуючи ці потужні математичні апарати, можна строго математично описати операції шифрування і дешифрування, і при цьому всі математичні перетворення будуть зрозумілими для інженерів-практиків.

З позицій теорії імпульсних систем і теорії керування ЛПМ з однією вхідною величиною $x[n]$ і з однією вихідною величиною $y[n]$ над полем Галуа $GF(p)$ може бути описана наступним чином

$$y[n] = \sum_{i=0}^{l} b_i x[n-i] - \sum_{i=1}^{m} a_i y[n-i], \quad GF(p), \tag{1}$$

де $a_i, b_i \in GF(p)$ – параметри ЛПМ.

Використовуючи апарат d-перетворення функціонування ЛПМ може бути представлено у вигляді передатної функції

$$J = \frac{Y}{U} = \frac{D[y(t)]}{D[u(t)]}, \tag{2}$$

де $u(t)$ - вхідна послідовність ЛПМ,

$y(t)$ - вихідна послідовність ЛПМ,

U - зображення $u(t)$,

Y - зображення $y(t)$.

Передатна функція по суті визначає алгоритм перетворення послідовності $u(t)$ в послідовність $y(t)$ або структуру ЛПМ при її апаратній реалізації. Метою криптоатаки може бути знаходження передатної функції ЛПМ, однак для цього необхідно мати $n + p^n$ початкових символів імпульсної функції $h(t)$, тобто всієї неперіодичної вихідної послідовності ЛПМ, яка генерується після переходу ЛПМ із початкового нульового стану.

Передатна функція, а також інші динамічні параметри (імпульсна функція, перехідна і частотна характеристики), хоча і спрощують аналіз поведінки ЛПМ, однак не можуть бути вичерпними характеристиками ЛПМ, оскільки отримані при нульових початкових умовах. Для підвищення крипостійкості ЛПМ необхідно встановлювати її в різні початкові стани, а його ідентифікація якраз і є метою більшості криптоатак. Тому для поглибленого дослідження властивостей ЛПМ необхідно ввести поняття керованості і спостережності загальної теорії керування. З цих позицій ЛПМ може бути представлена як кінцевий автомат лінійного типу, який над полем Галуа $GF(p)$ описується функцією станів (переходів)

$$S(t+1) = A \times S(t) + B \times U(t), \qquad GF(p)$$

і функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \qquad GF(p)$$

де t – дискретний час, $S(t)$, $U(t)$ и $Y(t)$ – відповідно вектори стану, вхідний і вихідний; A – основна характеристична матриця ЛПМ; B, C, D - характеристичні матриці ЛПМ.

На практиці найчастіше використовують ЛПМ над полем Галуа $GF(2)$, оскільки в криптографічних схемах найчастіше використовують лише два види РЗЛЗЗ:

- РЗЛЗЗ із зовнішнім суматором зворотних зв'язків, відомими також як регістри Фібоначчі;
- РЗЛЗЗ із внутрішніми суматорами зворотних зв'язків, відомими також як регістри Галуа.

Кожний вид РЗЛЗЗ є автономною ЛПМ, яка має такі особливості, що її характеристичні матриці B і D нульові або її вхідна послідовність $U(t)$ дорівнює нулю для всіх моментів часу $t \geq 0$ [5],[6].

Характеристичні матриці $A_{(F)}$ для регістрів Фібоначчі і $A_{(G)}$ для регістрів Галуа мають вигляд:

$$A_{(F)} = \begin{Vmatrix} 0 & 1 & 0 & \Lambda & 0 & 0 \\ 0 & 0 & 1 & \Lambda & 0 & 0 \\ 0 & 0 & 0 & \Lambda & 0 & 0 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & 0 & \Lambda & 0 & 1 \\ g_0 & g_1 & g_2 & \Lambda & g_{r-2} & g_{r-1} \end{Vmatrix}, \quad A_{(G)} = \begin{Vmatrix} 0 & 0 & 0 & \Lambda & 0 & g_0 \\ 1 & 0 & 0 & \Lambda & 0 & g_1 \\ 0 & 1 & 0 & \Lambda & 0 & g_2 \\ \Lambda & \Lambda & \Lambda & \Lambda & \Lambda & \Lambda \\ 0 & 0 & 0 & \Lambda & 0 & g_{r-2} \\ 0 & 0 & 0 & \Lambda & 1 & g_{r-1} \end{Vmatrix}. \qquad (3)$$

В матриці $A_{(F)}$ елементи останнього рядка та матриці $A_{(G)}$ елементи останнього стовпчика є коефіцієнтами породжувального багаточлена

$$G(x) = g_0 + g_1 x + g_2 x^2 + \Lambda + g_{r-2} x^{r-2} + g_{r-1} x^{r-1}, \qquad GF(2) \qquad (4)$$

Найважливішою характеристикою ЛПМ, яка використовуються в криптографії, є її здатність до генерування послідовностей псевдовипадкових чисел максимального періоду (M -послідовність). Існують два основних підходи до визначення умов отримання M -послідовності, причому в різних джерелах завжди розглядається лише один із них. Об'єднаємо ці два підходи.

Спочатку розглянемо співвідношення між примітивними багаточленами і багаточленами, що належать максимальному показнику.

ТВЕРДЖЕННЯ 1. Примітивний багаточлен $\varphi(x)$ степені n над полем Галуа $GF(p)$ є багаточленом, що належать максимальному показнику $p^n - 1$.

Відомо [5], що багаточлен $\varphi(x)$, який не ділиться на x, є дільником багаточлена $x^k + 1$ для деякого цілого числа k, тобто входить до розкладання багаточлена $x^k + 1$. Найменше таке додатнє число k називається показником, якому належить багаточлен $\varphi(x)$.

Відомо також [6], що всі примітивні багаточлени степені n входить до розкладання багаточлена $x^{p^n-1} + 1$ над полем Галуа $GF(p)$. Незвідний багаточлен степені n, який належить показнику $p^n - 1$, називається багаточленом, що належить максимальному показнику.

Отже, примітивний багаточлен $\varphi(x)$ степені n над полем Галуа $GF(p)$ є багаточленом, що належать максимальному показнику $k = p^n - 1$.

Непрямим доказом правильності твердження 1, є також той факт, що визначені експериментально примітивні багаточлени [8] входять до складу таблиць багаточленів, які належать максимальному показнику [5].

ТВЕРДЖЕННЯ 2. ЛПМ буде служити генератором M-послідовності, якщо породжувальний багаточлен (4) є або примітивним, або належить максимальному показнику $p^n - 1$.

Доведено [5], що ЛПМ розрядності n з матрицями A і B може генерувати послідовність псевдовипадкових чисел максимального періоду $2^n - 1$ (M-послідовність), якщо ЛПМ є n-керованою, тобто ранг матриці

$$L_n = \left\| A^{n-1}B, A^{n-2}B, \text{K}, AB, B \right\| \tag{5}$$

дорівнює n. Важливою характеристикою r-керованої ($r \le n$) ЛПМ є також існування вхідної послідовності не більше r, яка дозволяє перевести ЛПМ із стану $S(i)$ в стан $S(j)$ згідно рівняння

$$S(j) - A^r S(i) = L_r \left\| \begin{matrix} u(0) \\ u(1) \\ \Lambda \\ u(r-1) \end{matrix} \right\|. \tag{6}$$

З рівняння (6) при відомих характеристичних матрицях A і B і станах $S(i)$ і $S(j)$ можна визначити невідому вхідну послідовність $U(t) = u(0)u(1)\text{K}\,u(r-1)$, що може представляти інтерес для криптолога.

Цікавою властивістю ЛПМ є r-передбачуваність, яка дозволяє по відомим значенням входу в моменти часу t, $t-1$, ... , $t-r$ і виходу ЛПМ в моменти часу $t-1$, $t-2$, ... , $t-r$ визначити значення виходу ЛПМ момент часу t.

В сучасному потоковому шифруванні суть більшості відомих криптоатак спрямовано на визначення невідомого початкового стану РЗЛЗЗ, який відіграє роль секретного ключа, і при цьому вважаються, що супротивнику відомі структура зворотних зв'язків регістра та його вихідна послідовність. З позицій теорії ЛПМ така атака неявно використовує властивість спостережності ЛПМ. n-вимірну ЛПМ з характеристичними матрицями A і C, називають r-спостережною ($r \le n$), якщо ранг r має така матриця:

$$M_r = \left\| \begin{matrix} C \\ CA \\ \Lambda \\ CA^{r-1} \end{matrix} \right\|.$$

ЛПМ з характеристичними матрицями виду (3) є і n-керованими і n-спостережними.

Для окремих класів ЛПМ розроблені методи визначення її структури по відомій вихідній реакції. Наприклад, якщо для n-розрядного регістра Фібоначчі відома вихідна послідовність $Y(t)$ довжини $2n$, тоді за допомогою алгоритму Берлекемпа-Мессі [9] можна визначити еквівалентний РЗЛЗЗ мінімальної довжини, який буде генерувати ту ж вихідну послідовність.

Математичний апарат ЛПМ дозволяє підійти до задач потокового шифрування з різних позицій і досліджувати різні співвідношення між відомими та невідомими параметрами ЛПМ. В Таблиці 1 наведені можливі типові задачі визначення невідомих параметрів ЛПМ і необхідні при цьому умови.

В сучасній криптографії склалась думка при низьку стійкість потокових шрифтів на основі РЗЛЗЗ. Проведемо аналіз цього твердження з позицій математичного апарату ЛПМ. Прикладом класичної атаки, яка описана в багатьох підручниках, зокрема в [2], є атака по визначенню структури зворотних зв'язків n- розрядного РЗЛЗЗ при відомих $2n$ біт відкритого тексту і $2n$ біт зашифрованого тексту. В теорії керування вказану задачу можна сформулювати як задачу ідентифікації: по відомим вхідним і вихідним послідовностям визначити характеристичні матриці ЛПМ.

Ще одним відомим прикладом слабкості РЗЛЗЗ є його уразливість до атаки на основі вже згаданого раніше алгоритма Берлекемпа-Мессі. Можна згадати також багато інших успішних атак на РЗЛЗЗ [7]. Однак всі наведені приклади стосуються лише одного класу ЛПМ: регістрів Фібоначчі або регістрів Галуа. Головною причиною слабкості цього класу ЛПМ у відношенні до криптоатак є сильна розрідженість характеристичних матриць A, B, C, D. В задачі шифрування використовується лише

матриця A, яка має вигляд майже одиничної матриці. Фактично в сучасній криптографії потужний математичний потенціал ЛПМ використовується дуже поверхнево. Тому актуальною є розробка потокових шифрів на основі ЛПМ з малорозрідженими характеристичними матрицями A, B, C, D, які, зберігаючи високу швидкодію, мають значно більшу криптостійкість.

Таблиця 1 Задачі криптоаналізу з позицій теорії ЛПМ

Відомі параметри n-вимірної ЛПМ	*Невідомі параметри n-вимірної ЛПМ*	*Назва властивості ЛПМ*	*Додаткові умови*
1. Початковий стан $S(i)$ 2. Кінцевий стан $S(j)$ 3. Матриці A і B	Вхідна послідовність $U(t)$ або Вихідна послідовність $Y(t)$	r -керованість ($r \le n$)	1. Ранг матриці L_r дорівнює r 2. Довжина $U(t)$ і $Y(t)$ дорівнює r
1. Матриці A і C 2. Вихідна послідовність $Y(t)$	Початковий стан $S(0)$	r - спостережність ($r \le n$)	1. Ранг матриці M_r дорівнює r 2. Довжина $Y(t)$ дорівнює r
1. Попередня вхідна послідовність $U(t)$ 2. Попередня вихідна послідовність $Y(t)$	Наступна вихідна послідовність $Y(t)$	r - передбачуваність ($r \le n$)	1. Вхідна послідовність $U(t)$ в моменти часу $t, \dots, t-r$ 2. Вихідна послідовність $Y(t)$ моменти часу $t-1, \dots, t-r$
1. Вхідна послідовність $U(t)$ 2. Вихідна послідовність $Y(t)$	Матриці A, B, C, D	ідентифікованість	ЛПМ типу регістрів Фібоначчі або Галуа
1. Початковий стан $S(0)$ 2. Вихідна послідовність $Y(t)$	Матриця A ЛПМ з аналогічною вихідною послідовністю $Y(t)$	еквівалентність, подібність, ізоморфізм	1. ЛПМ типу регістрів Фібоначчі 2. Довжина $Y(t)$ дорівнює $2n$

Методи підвищення крипостійкості потокових шифрів

В теорії ЛПМ відомий багатоканальний аналог одноканальної, тобто традиційної ЛПМ [5]. Якщо одноканальна n-вимірна ЛПМ має характеристичні матриці A, B, C, D, тоді її f-канальний $(f \le n)$ аналог має такі характеристичні матриці A_f, B_f, C_f, D_f:

$$A_f = \left| A^f \right|; \qquad B_f = \left| A^{f-1}B, \text{K}\ , AB, B \right|;$$

$$C_f = \begin{vmatrix} C \\ CA \\ CA^2 \\ \Lambda \\ CA^{f-1} \end{vmatrix}; D_f = \begin{vmatrix} D & & & & \\ CB & D & & & \\ CAB & CB & D & & \\ \Lambda & \Lambda & \Lambda & \Lambda & \\ CA^{f-2}B & CA^{f-3}B & \Lambda & CB & D \end{vmatrix}.$$

Перевагою f-канальної ЛПМ є те, що за рахунок розпаралелення даних вона працює в f разів швидше, ніж одноканальна ЛПМ.

ПРИКЛАД. Для РЗЛЗЗ типу регістра Галуа, побудованого на основі породжувального багаточлена $P(x) = 1 + x + x^3$ характеристичні матриці одноканальної ЛПМ мають вигляд:

$$A = \begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix}, \quad B = \begin{vmatrix} 1 \\ 0 \\ 0 \end{vmatrix}, \quad C = \begin{vmatrix} 0 & 0 & 1 \end{vmatrix}, \quad D = \begin{vmatrix} 0 \end{vmatrix}. \tag{7}$$

Триканальна ЛПМ, аналогом якої є наведена вище одноканальна ЛПМ, буде мати такі характеристичні матриці:

$$A_3 = \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix}, \quad B_3 = \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix}, \quad C_3 = \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix}, \quad D_3 = \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{vmatrix}. \tag{8}$$

На Рис.1 наведена схема одноканальної ЛПМ, яка відповідає матрицям (7), а на Рис. 2 - схема триканальної ЛПМ у відповідності із матрицями (8).

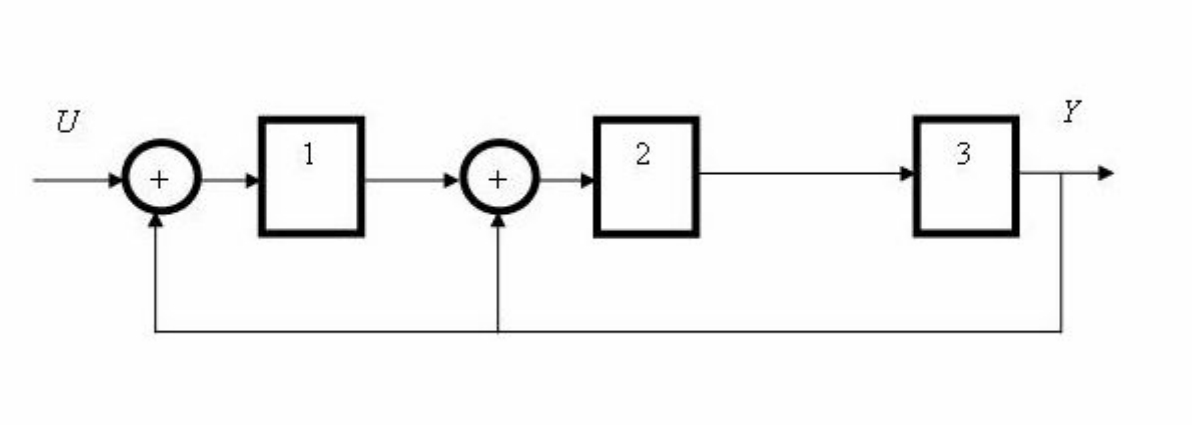

Рис. 1. Схема одноканальної ЛПМ

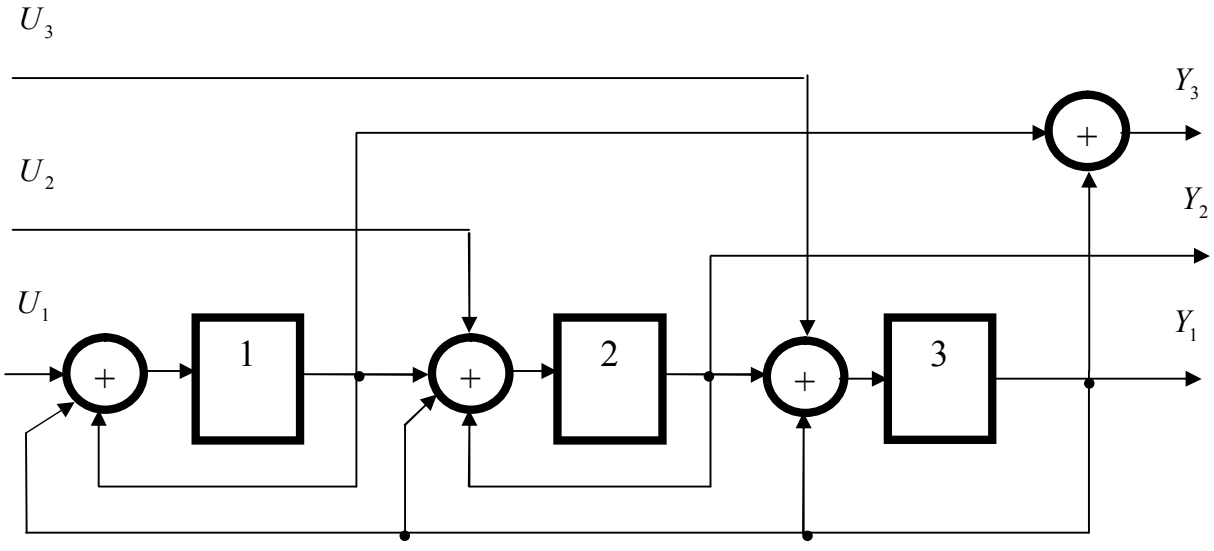

Рис. 2. Схема триканальної ЛПМ

Розглянемо криптографічні властивості f-канальної ЛПМ при умові що породжувальний багаточлен (4) її одноканального аналогу належить максимальному показнику. На всіх виходах такої f-

канальної ЛПМ генерується така ж M -послідовність, як і на виході одноканального аналогу, але із зсувом на відповідну кількість розрядів. Криптографічні властивості f -канальної ЛПМ можна значно підвищити, якщо використовувати не тільки всі її виходи, але і входи.

Розглянемо алгебраїчні властивості f -канальної ЛПМ P_f, створеної на основі одноканальної ЛПМ P з характеристичними матрицями A виду (3).

Властивість 1. Послідовність біт μ_k з виходу Y_k f -канальної ЛПМ P_f є M -послідовністю ($k = 1 \div f$).

Властивість 2. M -послідовність з виходу Y_k f -канальної ЛПМ P_f є циклічно зсунутою на визначену кількість w_k розрядів відносно M -послідовності з виходу одноканальної ЛПМ P.

Графовою моделлю ЛПМ P_f є сильнозв'язний граф $\Gamma = (V, E)$, де V - множина вершин, E - множина дуг з мітками $0,1,...,2^f - 1$ ($|V| = 2^n$, $|E| = 2^{n+f}$). Завдяки n -керованості ЛПМ P_f із вказаними характеристичними матрицями A_f, B_f, C_f, D_f, між будь-якими парами вершин v_i і v_j ($v_i, v_j \in V, i, j = 1 \div 2^n$) існує шлях не довше n. Якщо вийти із вершини v_i, то, прямуючи по дугам з однаковими мітками, можна знову повернутись у цю ж вершину v_i. Є 2^f таких шляхів однакової довжини ($2^n - 1$). Кожній вершині v_i графа Γ відповідає внутрішній стан $S(i)$ ЛПМ P_f, а кожній парі вершин v_i і v_j, з'єднаних дугою з міткою ρ ($\rho = 0 \div 2^f - 1$), відповідає перехід ЛПМ P_f із стану $S(i)$ в стан $S(j)$ при подачі на її вхід вектора $U(t)$ з кодом ρ.

Нехай перехід від стану $S(j)$ до стану $S(j+m)$ відповідає по графу Γ шлях із m дуг з однаковою міткою.

Властивість 3. M -послідовність з виходу Y_k при початковому стані $S(j+m)$ f -канальної ЛПМ P_f є циклічно зсунутою на m розрядів M -послідовністю з цього ж виходу про початковому стані $S(j)$.

Властивість 4. Для f -канальної n -вимірної ЛПМ P_f кількість N^f видів M -послідовностей на всіх її виходах над полем Галуа $GF(p)$ визначається величиною

$$N^f \le 2^n p .$$

Значення величини N^f визначається числом можливих циклічних зсувів основної M -послідовності та інверсної M -послідовності одноканального аналога ЛПМ P_f.

Порівняємо криптографічну стійкість гами, яка генерується для f незалежних паралельних каналів передачі даних двома варіантами: з використанням f окремих однакових одноканальних ЛПМ P та f -канальної ЛПМ P_f. Передбачається відомою структура зворотних зв'язків всіх ЛПМ.

В першому випадку для визначення невідомого початкового заповнення f одноканальних ЛПМ необхідно виконати по кожному каналу 2^n перебірних операцій, тобто складність обчислень дорівнює $O(f \cdot 2^n)$.

При використанні f -канальної ЛПМ P_f невідомим є як початковий стан ЛПМ, так і константний вхідний набір. Оскільки значення на всіх f виходах не є незалежними, тоді криптоаналітику необхідно перебрати всі варіанти початкового заповнення ЛПМ P_f для всіх варіантів константних вхідних наборів. Таким чином, складність обчислень дорівнює $O(2^f \cdot 2^n)$, тобто довжина секретного ключа складає ($f + n$) розрядів.

До f -канальної ЛПМ P_f не можна застосувати багато відомих криптоатак, які дозволяють за допомогою алгоритмів лінійної складності "зламати" одноканальну ЛПМ. Це, зокрема, стосується вже

згаданого алгоритму Берлекемпа-Мессі [9] і атаки по визначенню структури зворотних зв'язків при відомих $2n$ відкритого тексту і $2n$ біт зашифрованого тексту [2].

В сучасних потокових шифрах РЗЛЗЗ самостійно не використовуються, а лише служать базовими блоками в складі різних генераторів псевдовипадкових чисел. Введенням різних елементів нелінійності значно підвищується стійкість потокових шифрів до кореляційних та алгебраїчних атак [8].

За допомогою багатоканальної ЛПМ можна змоделювати роботу багатьох типів генераторів, в яких ефект нелінійності досягається змішуванням вихідних послідовностей від кількох РЗЛЗЗ. Найчастіше в таких генераторах один РЗЛЗЗ керує роботою інших РЗЛЗЗ.

Наприклад, в f-канальній ЛПМ P_f на один вихід Z_{ij} можна почергово видавати послідовності μ_i і μ_j з виходів відповідно Y_i і Y_j в залежності від сигналів послідовності μ_k з виходу Y_k по правилу:

$$Z(t) = \begin{cases} Y_i(t), & якщо\ Y_k(t) = 1 \\ Y_j(t), & якщо\ Y_k(t) = 0 \end{cases} . \qquad (9)$$

Для подвоєння періоду M-послідовності з виходу Z_{ij} можна через кожні $p^n - 1$ тактів змінювати у правилі (9) місцями виходи Y_i і Y_j. Для підвищення криптостійкості доцільно додатково змішувати M-послідовності з виходів Y_i і Y_j за допомогою нелінійних булевих функцій [10]. Якщо використати всі виходи f-канальної ЛПМ P_f в різних комбінаціях інформаційних та керуючих виходів, тоді можна отримати нелінійну гаму одночасно для f паралельних каналів передачі даних.

Висновки

Переважна більшість відомих схем потокового шифрування базується на використанні регістрів зсуву дуже простої структури, що дає підстави для помилкового твердження про недостатню стійкість потокового шифрування в цілому. Теоретичний базис ЛПМ дає не тільки глибоке розуміння суті відомих шифрів на основі РЗЛЗЗ, але і дозволяє розробляти більш складні і захищені криптографічні схеми. На основі потужної теорії ЛПМ можна описати операції шифрування і дешифрування і строго математично, і зрозуміло для інженерів-практиків.

На практиці часто виникає потреба в шифруванні багатоканальних систем передачі даних. Якщо використовувати для кожного каналу окремий генератор псевдовипадкових чисел, тоді виникає проблема в синхронізації всіх генераторів, а також необхідні значні додаткові апаратні витрати. При використанні одного генератора псевдовипадкових чисел почергово для всіх каналів виникають складнощі з отриманням високої частоти роботи генератора а також знижується загальна криптостійкість системи передачі даних.

Перевагою багатоканальних ЛПМ є можливість швидкісної обробки даних для паралельних каналів передачі даних із забезпеченням економії апаратних засобів і високої криптостійкості.

Список літератури

1. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н.Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. - 336 с.
2. Скляр Б. Цифровая связь.Теоретические основы и практическое применение. Изд. 2-е, испр. : Пер. с англ. - М.: Издательский дом "Вильямс", 2004. - 1004 с.
3. M. Hell and T. Johansson, "Two New Attacks on the Self-Shrinking Generator," *IEEE Trans. Inform. Theory*, vol. 52, pp. 3837-3843, No. 8, 2006.
4. S. Ronjom and T. Helleseth, "A New Attack on the Filter Generator," *IEEE Trans. Inform. Theory*, vol. 53, pp. 1752-1758, No. 5, 2007.
5. Гилл А. Линейные последовательностные машины: Пер. с англ. - М.: Наука, 1974. - 288 с.
6. Фараджев Р.Г. Линейные последовательностные машины. - М.: Сов. радио, 1975. - 248 с.
7. Schneier R. Applied Cryptography. New York: Wiley, 1996.
8. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. - 240 с.
9. Блейхут Р. Теория и практика кодов, исправляющих ошибки: Пер. с англ. - М.: Мир, 1986.-576 с.
10. Поточные шифры. Результаты зарубежной открытой криптологии. htpp://www.ssl.stu.neva.ru/psw/crypto.html

Семеренко Василь Петрович, к.т.н., доцент, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, Вінниця, 21021, Україна, тел.: (0432) 58-03-79, E-mail: sm@mail.vstu.vinnica.ua.

Степанишин Юрій, студент, Вінницький національний технічний університет, Хмельницьке шосе, 95, Вінниця, 21021, Україна, тел.: (0432) 58-03-79.

Гаєвський Максим, студент, Вінницький національний технічний університет, Хмельницьке шосе, 95, Вінниця, 21021, Україна, тел.: (0432) 58-03-79.