Використання узагальнених матриць Галуа і Фібоначчі у потокових шифрах

УДК 621.395.7 (043.2)

Арсен Ковальчук[1], Анатолій Білецький[2]

Національний авіаційний університет, [1]kovalchuk.arsen1@gmail.com, [2]abelnau@ukr.net

У доповіді розглянуто різні варіанти побудови двійкових генераторів псевдовипадкових послідовностей (ПВП) і алгоритмів потокового шифрування інформації на основі так званих узагальнених матриць Галуа і Фібоначчі. Терміни «матриця Галуа» і «матриця Фібоначчі» запозичена з теорії криптографії, в якій широко використовують генератори ПВП на регістрах зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) за схемою Галуа і Фібоначчі [1]. За допомогою матриць Галуа і Фібоначчі можна програмно обчислити такі ж самі бінарні послідовності, як і послідовності, які формують відповідні класичні РЗЛЗЗ-генератори ПВП.

Класичні матриці Галуа і Фібоначчі належать підмножині сильно розряджених матриць, тоді як узагальнені до підмножині щільних матриць. Перехід від класичних до узагальнених матричних генераторів ПВП супроводжується розширенням різноманіття генераторів, що призводить до істотного підвищення їхньої криптостійкості. Даний ефект досягається як за рахунок збільшення числа елементів, що утворюють матриці, так і за рахунок того, що узагальнені матриці синтезуються не тільки на основі примітивних породжувальних поліномів, а й на основі поліномів, які зовсім не обов'язково (як у класичних варіантах) є примітивними.

Матриці Галуа $\boldsymbol{G}$ і Фібоначчі $\boldsymbol{F}$ пов'язані оператором правостороннього транспонування (позначається символом $\perp$), що здійснює поворот матриці щодо допоміжної діагоналі. Якщо матриці $\boldsymbol{G}$ і $\boldsymbol{F}$ піддати класичному (лівосторонньому) транспонуванню (позначається символом T), то отримуємо так звані сполучені матриці Ґалуа та Фібоначчі.

Класичним генераторам і їхнім матричним еквівалентам притаманний істотний недолік, який полягає в тому, що вони схильні до атаки Берлекемпа-Мессі (БМ). Узагальнені матричні генератори ПВП вільні від атаки БМ. Остання властивість є наслідком такої особливості алгоритму БМ. Цим алгоритмом злому класичних РЗЛЗЗ-генераторів ПВП вирішується завдання обчислення єдиного невідомого - примітивного полінома, що породжує генератор. Для варіантів узагальнених матричних генераторів ПВП виникає необхідність у визначенні двох невідомих параметрів: як неприводного полінома, так і утворювального елемента, що спільно породжують узагальнену матрицю. Така проблема виявляється нерозв'язною для алгоритму Берлекемпа-Мессі [2], оскільки він призначений для обчислення лише одного невідомого параметра.

Результати досліджень узагальнено для розв'язання задач синтезу генераторів ПВП над полем Галуа непарних характеристик.

Розроблені матричні генератори ПВП стали основою побудови алгоритмів потокового шифрування інформації, один із варіантів якого наведено на рис. 1.

Результати статистичних випробувань шифру пакетом NIST STS підтвердили високу ефективність криптографічного захисту вихідних текстів.

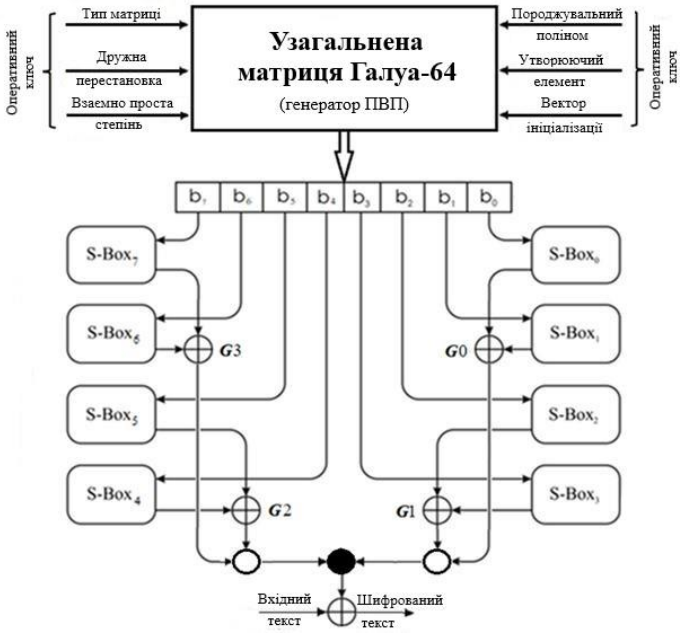

Рис. 1. Структурно-логічна схема поточного шифру

Оператори ○ та ● незалежно один від одного реалізують перетворення: порозрядного складання(0) або конкатенації (1) так, що шифруючи гама приймає значення наведене на рис. 2.

№	○	●	Перетворення	Довжина гами
1	0	0	$(G_0 \oplus G_1) \oplus (G_2 \oplus G_3)$	1 байт
2	0	1	$(G_0 \oplus G_1) \| (G_2 \oplus G_3)$	2 байта
3	1	0	$(G_0 \| G_1) \oplus (G_2 \| G_3)$	2 байта
4	1	1	$(G_0 \| G_1) \| (G_2 \| G_3)$	4 байта

Рис. 2. Варіанти шифрування гами

1. Anatoly Beletsky. Generalized Galois-Fibonacci Matrix Generators Pseudo-Random Sequences. *I. J. Computer Network and Information Security*, 2021, 6, pp. 57-69.
2. Anatoly Beletsky. Generalized Galois and Fibonacci Matrices in Cryptographic Applications. *WSEAS Transactions on Circuits and Systems*, Vol. 21, 2022, pp. 1-19.