УДК 004.421.5

В.М. Галів, аспір.
С.М. Іщеряков, к.т.н., доц.
Івано-Франківський національний технічний університет нафти і газу

МЕТОД ГАМУВАННЯ ЦИФРОВИХ ДАНИХ БАГАТОРІВНЕВИМИ ПСЕВДОВИПАДКОВИМИ ПОСЛІДОВНОСТЯМИ

У роботі запропонований метод криптографічної обробки інформації на основі гамування цифрових даних багаторівневими лінійними рекурентними послідовностями максимальної довжини із використанням суматора із змінним модулем перерахунку, на виході якого фактично формується вийняток від суми двох чисел. Наведена структура апаратного пристрою для реалізації запропонованого методу.

Гамування – один з найвідоміших і найпоширеніших методів криптографічної обробки інформації. Відомі методи криптування гамуванням базуються на бінарних псевдовипадкових послідовностях максимальної довжини (М-послідовностях) і побудовані на основі суматорів (програмних чи апаратних) за модулем 2. Розширення ансамблю псевдовипадкових послідовностей збільшує рівень криптостійкості таких систем. Одним з методів розширення ансамблю є застосування в якості кодуючої послідовності багаторівневих М-послідовностей.

Запропонований метод реалізується на основі суматора із змінним модулем перерахунку, на виході якого фактично формується вийняток (рос. – вычет) від суми двох чисел.

Розглянемо способи гамування двійкової інформаційної послідовності бінарними та багаторівневими М-послідовностями.

Бінарне гамування полягає в побітовому додаванні кодуючої та інформаційної послідовностей за модулем 2 програмними чи апаратними засобами. В результаті гамування одержується закодована послідовність, розшифровка котрої можлива тільки за допомогою зворотньої операції повторного додавання закодованої послідовності з кодуючою послідовністю за модулем 2. Як приклад розглянемо гамування інформаційної послідовності *inf* 5CD349 кодуючою послідовністю *code* довжиною $L = 2^4 - 1 = 15$ (111100010011010).

Inf	0101	1100	1101	0011	0100	1001
			mod 2			
Code	1111	0001	0011	0101	1110	0010
Res	1010	1101	1110	0110	1010	1011
Res hex	A	D	E	6	A	B

Результатом кодування інформації є послідовність *Res* ADE6AB (hex).

Кодування бінарним гамуванням можливе єдиним способом. При використанні в якості кодуючих послідовностей багаторівневих М-послідовностей, виникає неоднозначність в методах гамування. Нижче розглянуті два методи гамування бінарних даних багаторівневими М-послідовностями:

1) додавання за модулем 2 (упаковане і неупаковане);
2) додавання за довільним модулем.

Суть першого методу полягає в побітовому додаванні багаторівневої кодуючої та бінарної інформаційної послідовностей за модулем 2. Для цього багаторівнева М-послідовність записується як неупакована бінарна послідовність, представлена тетрадами, байтами, словами, тощо . Як і у випадку з бінарними кодуючими послідовностями, закодована послідовність отримується шляхом додавання інформаційної послідовності з кодуючою за модулем 2. Наприклад, в результаті гамування даних *inf* 5CD349E2C3 неупакованою кодуючою послідовністю *code* довжиною $L = 3^3 - 1 = 26$ (22102220010121120111002021) одержимо:

Inf	0101	1100	1101	0011	0100	1001	1110	0010	1100	0011
					mod 2					
Code	0010	0010	0001	0000	0010	0010	0010	0000	0000	0001
Res	0111	1110	1100	0011	0110	1011	1100	0010	1100	0010
Res hex	7	E	C	3	6	B	C	2	D	2

Відмінність методу гамування із застосуванням упакованих багаторівневих М-послідовностей від попереднього полягає в упаковці (відкиданні нулів у старших розрядах) символів кодуючої послідовності. Для тих самих інформаційної та кодуючої послідовностей одержимо:

Inf	01 01	11 00	11 01	00 11	01 00	10 01	11 10	00 10	11 00	00 11
					mod 2					
Code	10.10	01.00	10.10	10.00	00.01	00.01	10.01	01.10	00.01	01.01
Res	11 11	10 00	01 11	10 11	01 01	10 00	01 11	01 00	11 01	01 10
Res hex	F	8	7	B	5	8	7	4	D	6

Слід відмітити, що при використанні кодуючих послідовностей з основами, які у двійковому представленні мають 4, 8, 16 і т.д. біт, упакований та неупакований варіанти першого методу співпадають.

Представлення багаторівневої послідовності неупакованою бінарною супроводжується великою кількістю нулів в старших розрядах. Тому упаковане представлення багаторівневих послідовностей є більш ефективним для кодування інформаційних потоків.

Суть методу гамування за довільним модулем полягає в посимвольному додаванні інформаційної та кодуючої послідовностей за модулем $mod > 2$. При цьому бінарна інформаційна послідовність перед криптуванням представляється символами з основою $p_{inf} > 2$. Модуль перерахунку mod обирається рівним значенню більшої основи:

$$mod = \begin{cases} p_{inf} & \text{при } p_{inf} > p_m, \\ p_m & \text{при } p_{inf} < p_m, \end{cases}$$

де p_m – основа кодуючої послідовності.

Як приклад додамо за модулем 16 попередні інформаційну та кодуючу послідовності:

Inf	5	C	D	3	4	9	E	3	D	3
					mod16					
Code	2	2	1	0	2	2	2	0	0	1
Res hex	7	E	E	3	6	B	1	3	D	4

Інформаційна послідовність може бути представлена і за іншим модулем, наприклад 4:

Inf	1 1	3 0	3 1	0 3	1 0	2 1	3 2	0 3	3 1	0 3
					mod 4					
Code	2 2	1 0	2 2	2 0	0 1	0 1	2 1	1 2	0 1	1 1
Res	3 3	0 0	1 3	2 3	1 1	2 2	1 3	1 1	3 2	1 0
Res hex	F	0	7	B	5	A	7	5	E	4

Декодування інформації відбувається шляхом віднімання кодуючої послідовності від закодованої за тим модулем, за яким здійснювалось кодування інформаційної послідовності.

На рис.1 наведена структура пристрою для кодування інформаційного бінарного потоку багаторівневою М-послідовністю. Пристрій містить три основні елементи : перетворювач бінарного послідовного потоку у паралельно-послідовний потік змінної розрядності, генератор багаторівневих М-послідовностей, суматор за змінним модулем.

Перетворювач бінарного послідовного інформаційного потоку serial inf у паралельно-послідовний потік inf змінної розрядності r, структурна схема якого наведена на рис.2, реалізований на основі послідовного регістру зсуву SRG. Реверсивний лічильник CT із паралельним записом даних забезпечує зміну розрядності паралельних інформаційних відліків inf, що формуються на виході регістру зсуву SRG і перезаписуються до вихідного паралельного регістру PRG. Очевидно, що частота формування потоку паралельних інформаційних відліків на виході перетворювача в r разів нижча від частоти F надходження бітів вхідного потоку.

Паралельні коди інформаційного відліку inf та символу багаторівневої М-послідовності cod надходять на входи суматора за змінним модулем mod, до складу якого входять (рис. 3) два двійкових r-розрядних суматора 1 і 5, цифровий r-розрядний компаратор 2, логічний елемент ЧИ-НЕ 3, а також *r*-розрядний клапан 4 на основі логічних елементів ЧИ-НЕ. (R+1) – розрядна

сума паралельних кодів інформаційного відліку inf та символу М-послідовності cod порівнюється із r-розрядним значенням модуля перерахунку mod.

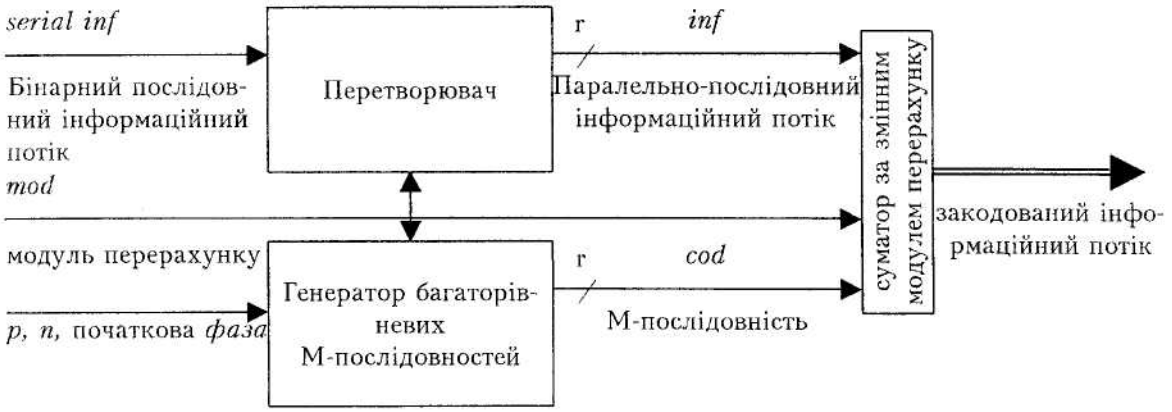

Рис. 1. Структура пристрою гамування бінарного потоку багаторівневими М-послідовностями

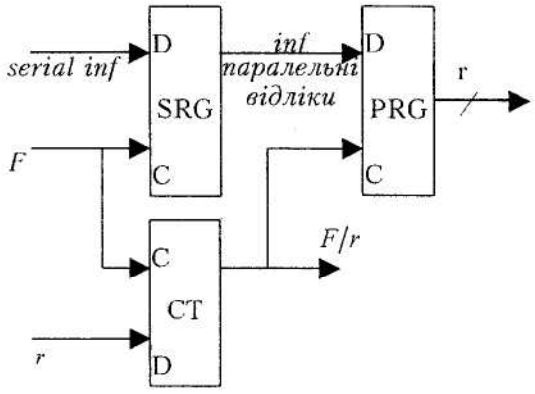

Рис. 2. Структура перетворювача бінарного послідовного інформаційного потоку serial inf у паралельно-послідовний потік inf змінної розрядності r

Якщо отримана сума менше модуля перерахунку:

$$\text{inf} + \text{cod} < \text{mod}, \tag{1}$$

то клапан 4 є закритим. Вихідний нульовий сигнал на виході закритого клапана 4 забезпечує проходження закодованого відліку, який не перевищує модуля перерахунку, з виходу суматора 1 через суматор 5 без змін.

При невиконанні умови (1) значення модуля перерахунку mod проходить через відкритий клапан 4 і в інвертованому вигляді надходить на вхід суматора 5, який фактично виконує функцію віднімання (inf + cod) − mod.

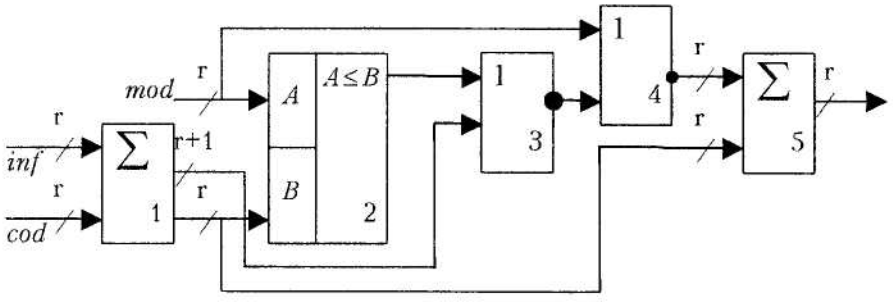

Рис. 3. Структура суматора за змінним модулем

Керування станом клапана 4 здійснюється вихідним сигналом логічного елементу ЧИ-НЕ 3. Нульовий сигнал на виході логічного елементу 3, який відкриває клапан 4, формується або при наявності одиничного старшого (r + 1)-го розряду суми інформаційної та кодуючої послідовностей, або при невиконанні умови (1) r-розрядною сумою.

Основою генератора багаторівневих М-послідовностей, структура якого наведена на рис.4, є n-каскадний регістр зсуву 1, кожен каскад якого містить паралельний двійковий код одного символу М-послідовності.

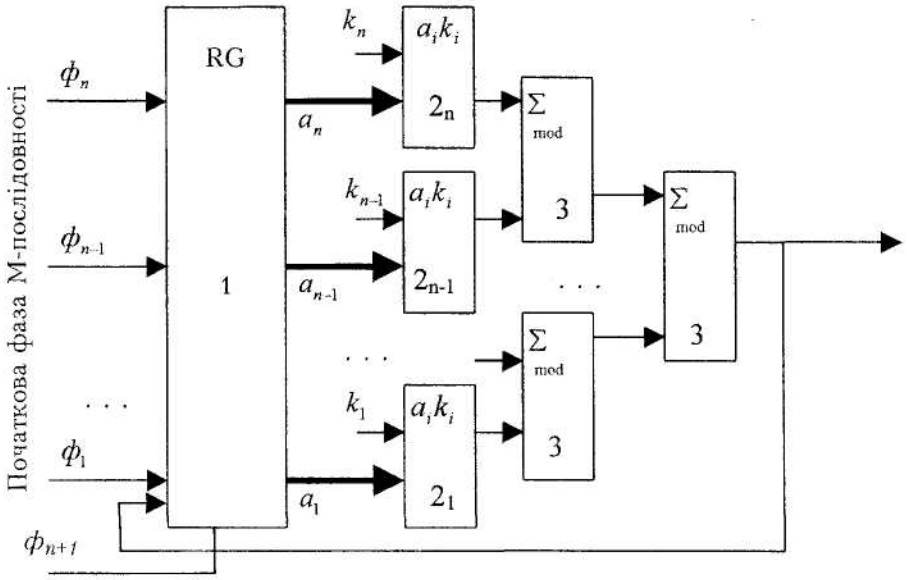

Рис. 4. Структура генератора багаторівневих М-послідовностей

Кількість r бітів ($r \geq \log_2 p_{\max}$) в кожному каскаді обирається максимально можливою для забезпечення генерування М-послідовності з щонайбільшою основою $p_{\max}$. Для визначеності представимо 8-розрядний каскад (r = 8), в якому можуть генеруватися М-послідовності з основою p = 2, 3, ..., 251. Зсув всередині регістру відбувається не побітово, а посимвольно (для обраного прикладу – по 8 біт.)

Кількість n каскадів в регістрі також обирається максимально можливою для звбезпечення геперування М-послідовності щонайбільшої довжини $l_{\max} = p_{\max}^{n_{\max}} - 1$.

Наприклад, при використанні 64-каскадного регістру зсуву, генератор забезпечить генерування М-послідовностей від $2^2 - 1$ до $251^{64} - 1$.

Запис значення початкової фази також здійснюється посимвольно шляхом паралельного запису до регістру n паралельних кодів символів $\phi_1 ... \phi_n$ М-послідовності.

Кожному i-му ($i = 1..n$) каскаду регістру зсуву 1 в схемі генератора відповідає модульний помножувач 2_i, на перший вхід якого надходить паралельний код одного символу n-символьного фрагменту $a_1 ... a_n$ М-послідовності, що зберігається в регістрі зсуву.

На другий вхід кожного i-того модульного помножувача надходить паралельний код коефіцієнту k_i неприведеного примітивного поліному, що утворює М-послідовність:

$$a_{n+1} = (a_n k_n) \bmod p + (a_{n-1} k_{n-1}) \bmod p + ... + (a_1 k_1) \bmod p .$$

Принцип функціонування модульного помножувача, структура якого наведена на рис. 5, базується на очевидній залежності:

a mod p + a mod p = (2a) mod p при a ≤ p.

Основою модульного помножувача є лінійка з $r - 1$ r-розрядних модульних суматорів, кожен з яких (рис. 6) є спрощеним варіантом модульного суматора, представленого раніше на рис. 3.

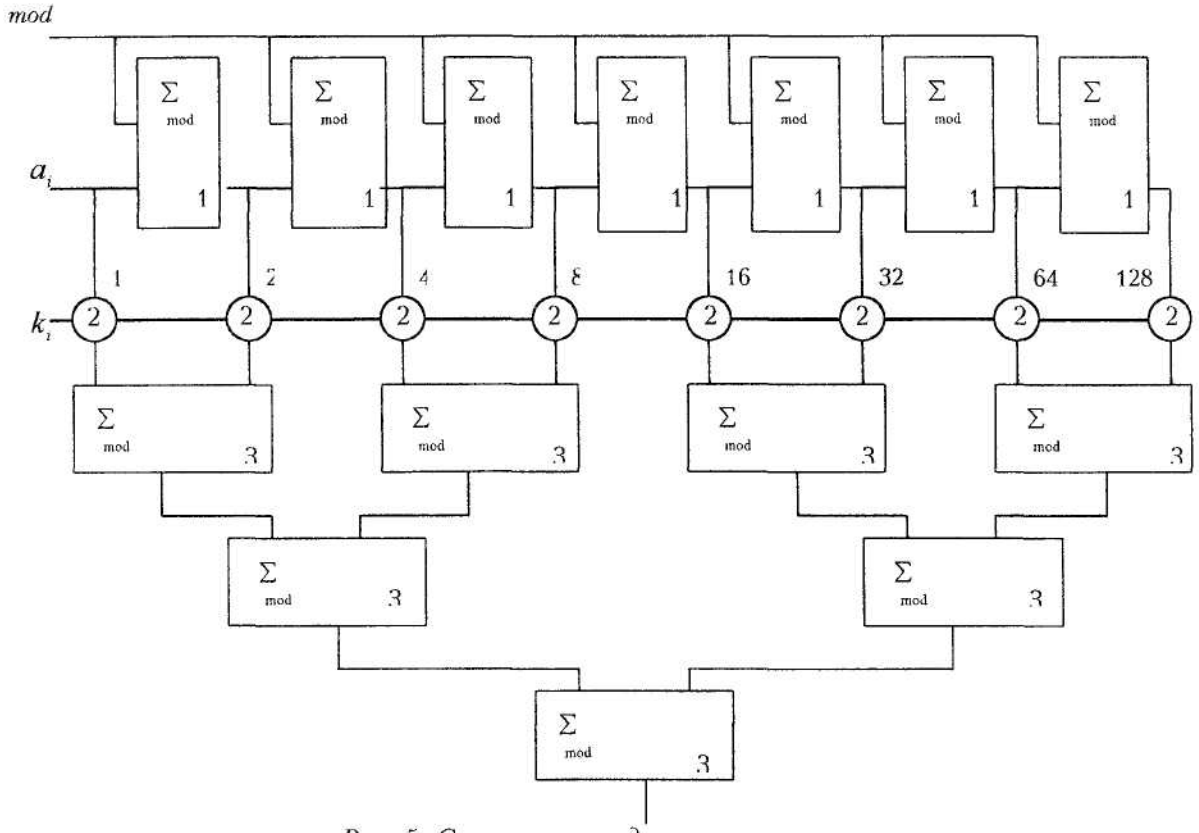

Рис. 5. Структура модульного помножувача

На виходах кожного j-того модульного суматора 1_j, зображеного на рис. 6 ($j = 1...r-1$) формується модульне значення часткового множника, що відповідає двійковому розряду 2^j. Отримане модульне значення 2^j надходить на інформаційний вхід відповідного ключа 2. Керуючий вхід ключа відповідає біту 2^j паралельного коду коефіцієнта k_i утворюючого полінома.

Пірамідальна схема включення модульних суматорів 3, кожен з яких є повністю аналогічним схемі, зображеній на рис. 2, забезпечує формування на виході помножувача модульного добутку $(a_i k_i) \bmod p$.

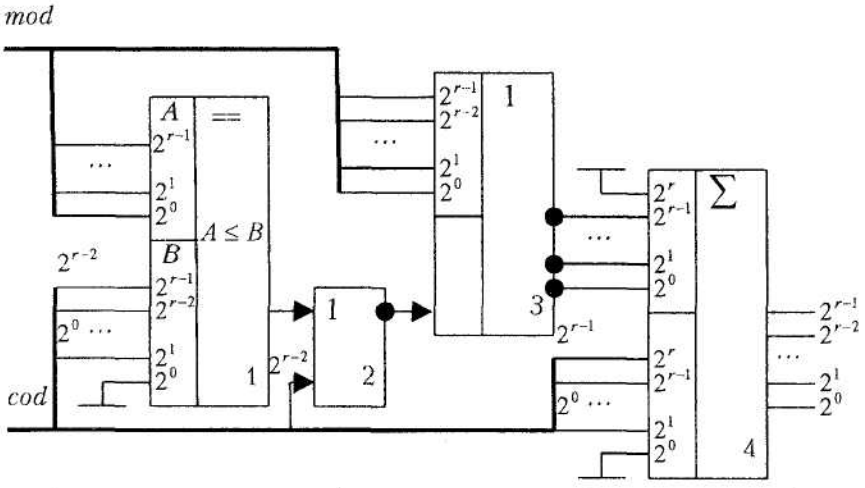

Рис. 6. Структура модульного суматора для визначення (2a) mod p

(N + 1)-й символ М-послідовності (рис. 4) утворюється шляхом модульного додавання паралельних кодів з виходів помножувачів $2_1...2_n$ також за допомогою пірамідальної структури модульних суматорів 3, схема яких аналогічна рис. 3.

Розроблена схема генератора є універсальною, а в наслідок цього надлишковою при використанні основ та довжин М-послідовностей далеких від максимально можливих. Проте, наявність нулів в старших каскадах регістру (при незначних довжинах) та в старших розрядах каскадів (при незначних основах) не впливає на якість роботи схеми.

Запропонований метод гамування двійкових даних багаторівневими М-послідовностями дозволяє підвищити криптостійкість систем не тільки за рахунок розширення ансамблю бінарних кодуючих послідовностей багаторівневими. Можливість зміни модуля гамування, яка, в свою чергу, може відбуватись в реальному часі по псевдовипадковому закону, забезпечує багаторазове зростання рівня криптостійкості систем передавання даних.

ГАЛІВ Василь Михайлович – аспірант Івано-Франківського національного технічного університету нафти і газу.

Наукові інтереси:

– застосування псевдо випадкових послідовностей.

Тел.: (0342) 523315.

E-mail: vgal@ukr.net

ІЩЕРЯКОВ Сергій Михайлович – кандидат технічних наук, доцент кафедри прикладної математики Івано-Франківського національного технічного університету нафти і газу.

Наукові інтереси:

– цифрова обробка сигналів.

Тел.: (03422) 42127.

E-mail: ism@ac.ifdtung.if.ua

Подано 20.08.2002.