де $\|Gal\|$ – матриця розміру $N\times n$ системи Ґалуа; $\|W\|$ – матриця розміру $N\times N$ рекурсивно впорядкованих функцій Уолша; $\|R\|$ – матриця розміру $N\times n$ відображеної вагової мережі Радемахера.

Для прикладу, матрична операція переходу від функцій Уолша до функцій Ґалуа та матриця розміру 8×8 дискретних значень функцій Ґалуа в полі $GF(2^3)$ з породжуючим вектором 1101 згідно процедури рекурсивного розширення подаються відповідно

$$\begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} = \begin{Vmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & 1 \end{Vmatrix} \longrightarrow \begin{Vmatrix} 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 \end{Vmatrix}.$$

При дискретизації за параметром часу перших n функцій Ґалуа та здійсненні бінарної заміни значень функцій 1 на 0, –1 на 1, згідно виразу

$$g_k(\theta_s)=(1-Gal(n-k-1,\theta_s))/2,$$

одержують матрицю кодових елементів Ґалуа розміру $n\times N$, $k=0,1,\ldots,n-1$.

При дискретизації системи N функцій Ґалуа $\{Gal(n,\theta,i)\}$, $i=0,1,\ldots.2^n-1$ та перетворенні значень функцій отримують повну матрицю кодових елементів Ґалуа розміру $N\times N$, впорядкованих із поелементним рекурсивним зсувом згідно другої діагоналі матриці Ґалуа. Номер s повідомлення однозначно визначається n-координатним вектором $n=log_2 N$.

Висновок

Використання властивості рекурентності базису Галуа в наш час склало фундаментальну основу розробки теорії та принципово нових технічних рішень багатьох складних задач і практичних застосувань у галузі цифрового формування, передавання і опрацювання інформаційних потоків, в тому числі при побудові кодових систем Галуа, кодових шкал Галуа, розробці баз даних та нових методів передавання інформації в умовах інтенсивних завад.

Список використаних джерел

1. Николайчук Я.М. Коди поля Галуа : теорія і застосування – Тернопіль: ТзОВ "Терно–граф", 2012. – 576 с.
2. Николайчук Я.М. Теорія джерел інформації - Тернопіль: ТзОВ «Терно-граф», 2010.- 536с.

УДК 681.3

СИСТЕМА ЗАХИСТУ МАНІПУЛЬОВАНИХ ДАНИХ В БАЗИСІ ГАЛУА

Николайчук Я.М.[1)], Шкодін О.В.[2)]
Тернопільський національний економічний університет
[1)] д.т.н., професор; [2)] магістрант

І. Постановка задачі

Сучасні тенденції розвитку пакетної передачі даних в мережі, потребують передавання інформації з максимальною швидкістю на максимальну відстань, із виправленням помилок і із захистом від несанкціонованого доступу. У зв’язку з цим актуальним є питання ефективного маніпулювання сигналів в базисі Галуа.

II. Мета роботи

Метою дослідження є переваги в маніпуляції даних у базисі Галуа, яка дозволить збільшити якість даних, які передаються, а також забезпечить захист від несанкціонованого доступу.

III. Принципи обробки і формування даних, які забезпечують виправлення помилок на основі сигнальних коректуючи кодів поля Галуа

Коди поля Галуа (1) в загальній класифікації відносяться до підкласу циклічних блочних кодів, які володіють всіма властивостями захищених кодів. В блочних кодах послідовність елементарних повідомлень розбиваються на блоки символів ($B_1,B_2,B_3,\ldots B_n$) фіксованої довжини, до кожного з яких ставиться у відповідність певна комбінація символів кодового слова ($b_1,b_2,b2\ldots,b_n$).

Для генерації кодів поля Галуа $G(2^n)$ використовуються примітивні алгебраїчні многочлени:

$$4{:}x_1 \oplus x_4;\ 5{:}\ x_2 \oplus x_5;\ 6{:}x_1 \oplus x_6;\ 7{:}\ x_3 \oplus x_7;\ 8{:}x_2 \oplus x_3 \oplus x_4;\ 9{:}\ x_4 \oplus x_9;\ 10{:}x_3 \oplus x_{10};\ 11{:}\ x_2 \oplus x_{11};$$
$$12{:}x_1 \oplus x_4 \oplus x_6 \oplus x_{12};$$
$$13{:}\ x_1 \oplus x_3 \oplus x_4 \oplus x_{13};\ 14{:}x_1 \oplus x_6 \oplus x_{10} \oplus x_{14};\ 15{:}\ x_1 \oplus x_{15};\ 16{:}x_1 \oplus x_3 \oplus x_{12} \oplus x_1 6;\ 17{:}\ x_3 \oplus x_{17};\ 18{:}x_7 \oplus x_{18}; \quad (1)$$
$$19{:}\ x_1 \oplus x_2 \oplus x_5 \oplus x_{19};\ 20{:}x_3 \oplus x_{20};\ 21{:}\ x_2 \oplus x_{21};\ 22{:}\ x_1 \oplus x_{22};\ 23{:}x_5 \oplus x_{25};\ 24{:}x_1 \oplus x_3 \oplus x_4 \oplus x_{24};$$
$$25{:}\ x_3 \oplus x_{25};\ 26{:}x_1 \oplus x_2 \oplus x_6 \oplus x_{26};\ 27{:}\ x_1 \oplus x_2 \oplus x_5 \oplus x_{27};\ 28{:}x_3 \oplus x2_8;\ 29{:}\ x_2 \oplus x2_9;\ 30{:}x_1 \oplus x_4 \oplus x_6 \oplus x_{30};$$
$$31{:}\ x_7 \oplus x_{31};\ 32{:}x_2 \oplus x_6 \oplus x_{32};$$

Існують також примітивні алгебраїчні многочлени для полів більш високих порядків $G\begin{pmatrix} n \\ p \end{pmatrix}$, де p – просте число. Важливою перевагою кодової послідовності Галуа являється проста генерація кодів на основі рекурентного рівняння. Простійші ключі кодів Галуа описуються виразом:

$$G_i = G_{i-1} \oplus G_{i-m}; \qquad m \le n. \quad (2)$$

Важливою математичною і практичною властивістю в послідовності Галуа є наявність різнорівневих рекурсивних зв'язків, які мають високі ентропійні характеристики. Кодування даних на основі кодової послідовності Галуа показано на рис. 1:

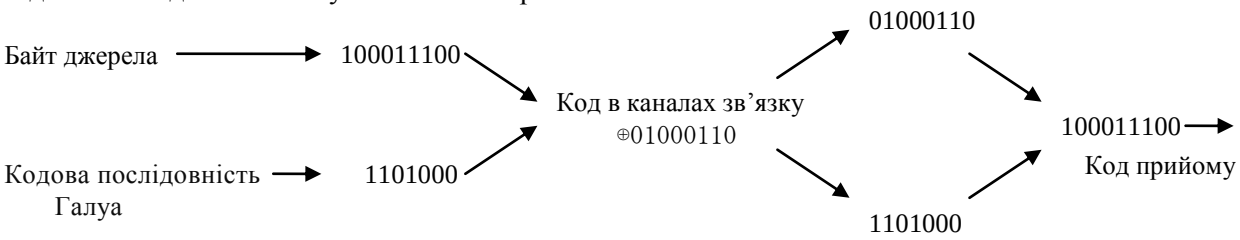

Рисунок 1 – Кодування даних на основі послідовності Галуа

При передачі і прийомі інформації на основі запропонованих кодів маніпульовані сигнали формуються на основі чотирьох ознак (↑, ↓, +, –), які поставлені в відповідності елементам інформаційного повідомлення, відповідно кодам поля Галуа. Принцип формування сигнального коректуючого коду поля Галуа полягає у тому, що біти одиниць в пакетів даних нумерується рекурентним кодом поля Галуа $G\begin{pmatrix} n \\ 2 \end{pmatrix}$. При чому для одиниць в пакеті даних біт Галуа 1 передається фронтом наростання (↑), а біт Галуа 0 передається фронтом спаду (↓). Біти нулів в пакеті даних також нумерується рекурентним кодом поля Галуа $G\begin{pmatrix} n \\ 2 \end{pmatrix}$. Для нулів в пакеті даних біт 1 передається потенціалом + (плюс), а біт Галуа 0 передається потенціалом – (мінус).

На рис. 2 показана схема реалізації знаходження і виправлення помилок кодовано-маніпульованих сигналів на фізичному рівні, де N номер позиції бітів в інформаційному повідомленні; Д – інформаційні біти прийнятих даних з виявленими і виправленими помилками; CrK – сигнальний код;

$G_2^4(1), G_2^4(0)$ - відповідно біти Галуа G_2^4 для інформаційних бітів 1 і 0 з виявленням і виправленням помилок; 0*,1* - помилкові біти.

№ Біти	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
СгК																								
$G_2^4(1)$	1			1		1		1	0	0* /1		0	1		1	0		1	0	0	1* /0		0	
$G_2^4(0)$		1	1		1		0 * / 1				0			1			1* /0					1		1
Д	1	0	0	1	0	1	0	1	1	1	0	1	1	0	1	1	0	1	1	1	1	0	1	0

Рисунок 2 – Схема реалізації виявлення і виправлення помилок кодовано маніпульованих сигналів

Можливі тільки випадки ідентифікації бітів Галуа: інвертування біту Галуа - ознака одиничного чи нульового біту і заміна сигнальних ознак ↑, ↓ на длюс (+), мінус (-) чи навпаки. У всіх випадках помилка знаходиться і повинна виправлятись програмно-апаратним декодером Галуа.

Висновки

Дана технологія кодованої маніпуляції сигналів на фізичному рівні комп'ютерних мереж являється сумісною з відомими стандартними протоколами. Разом з технологією розпізнання гармонічних сигналів дозволяє збільшити швидкість передачі інформації на низових рівнях в умовах впливу інтенсивних перешкод.

Список використаних джерел

1. Николайчук Я.М. Коди поля Галуа: теорія та застосування. – Тернопіль: ТзОВ «Терно-граф», 2010 – 536с.
2. Николайчук Я.М., Заведюк Т.О. Структура та функції рекурентного біонейрона для розпізнання образів у Хеммінговому просторі // Поступ в науку. – 2010 - №6 – с. 37-39
3. Nykolaychuk Y.M. Voronych A.R. Entropic methods of signal processing with protection from errors in Galios base // J.Qafqaz Univ. – Baku, 2010 – N 30 – P 69 – 77

УДК 004.318

ОЦІНКА МЕТОДИЧНОЇ ПОХИБКИ МЕТОДУ ВИМІРЮВАННЯ СЕРЕДНЬОЇ ЕНЕРГІЇ СПОЖИВАННЯ МІКРОПРОЦЕСОРІВ

Осолінський О.Р.

Тернопільський національний економічний університет, аспірант

І. Постановка проблеми

Оптимізація програмного забезпечення вбудованих систем за енергоспоживанням вимагає побудови адекватних моделей енергоспоживання мікропроцесора. Їх побудова ускладнюється характером процесу споживання енергії мікропроцесором – він складається з піків, синхронних до змін стану тактового генератора. В [1] запропоновано систему вимірювання миттєвої потужності споживання мікропроцесорів при виконанні окремих інструкцій, яка має ряд суттєвих переваг перед відомими – мікропроцесор працює в штатному режимі, відповідна методика корекції похибок дає змогу отримати похибку вимірювання не більше 0,75%. Однак експериментальні дослідження показали, що система [1], через вимірювання миттєвих значень напруги, має низьку завадостійкість.

Вказаний недолік усунуто в системі [2], що використовує при вимірюванні метод двохтактного інтегрування, а, з метою підвищення точності порівняння результатів вимірювання обома системами, система, описана в [2], використовує більшість елементів, від яких залежить похибка вимірювання, системи [1]. Тому похибка порівняння результатів вимірювання менша похибки вимірювання.

Однак при синтезі структури системи [2] зроблено припущення, що, при умові $\int_0^T \Delta u dt \to 0$, де

Δu – відхилення поточної напруги живлення мікропроцесора u від номінальної U_{REF} , а T – час