УДК 004.382

Р. М. Еліас[1], В. С. Глухов[2], М. Рахма[2], І. М. Жолубак[2]
[1]Ліванський міжнародний університет,
кафедра електротехніки та електронної інженерії
[2]Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

ВБУДОВАНИЙ КОНТРОЛЬ ПРИСТРОЇВ ДЛЯ ОПРАЦЮВАННЯ ЕЛЕМЕНТІВ РОЗШИРЕНИХ ПОЛІВ ГАЛУА

Двійкові коди елементів розширених полів Галуа є надлишковими, частина з них ніколи не з'являються при нормальній роботі пристроїв опрацювання елементів таких полів. Невикористані (заборонені) кодові комбінації можна задіяти для робочого діагностування (вбудованого контролю) цих пристроїв. Ознакою помилки буде поява будь-якої забороненої комбінації. У роботі порівнюються різні розширені поля Галуа за можливістю організації робочого діагностування, визначаються поля, які якнайкраще забезпечують його проведення. Зазначено, що для кодів елементів полів Галуа не існує бітів, які мають суворо різні значення в дозволених та заборонених кодах. Можливість діагностування пропонується оцінювати відношенням кількості заборонених комбінацій до загальної кількості комбінацій або до кількості дозволених комбінацій. Для досягнення найбільшого ефекту діагностування рекомендується використовувати поля з характеристиками, які є першим простим числом, більшим за степінь 2. З погляду ціни діагностування, найкращим є поле $GF(3^m)$, для якого необхідно визначати лише одну заборонену кодову комбінацію, що забезпечує виявлення усіх заборонених кодів. З використанням розглянутих полів Галуа $GF(d^m)$ мінімальна кодова відстань для кодів кожної цифри коду дорівнює 1. Це вказує на те, що виявити 100 % усіх навіть поодиноких помилок у роботі розглянутих пристроїв запропонованим способом неможливо. Пошук логічного виразу для позначення помилки ґрунтується на поділі групи послідовних заборонених кодів на підгрупи. Для кожної підгрупи розряди її кодів ділять на дві частини так, щоб старші розряди кожного коду з підгрупи залишалися незмінними, а молодші - пробігали всі значення від 0...0 до 1...1. Тоді до мінімізованого логічного виразу помилки у цій підгрупі кодів увійдуть тільки незмінні старші розряди. Апаратна складність запропонованого методу квадратично залежить від кількості бітів, якими кодується один розряд коду елементів розширених полів Галуа.

Ключові слова: розширені поля Галуа, ємнісна складність, вбудоване тестування.

Rodrigue Elias[1], Valerii Hlukhov[2], Mohammed Rahma[2], Ivan Zholubak[2]

[1]Lebanese International University,
Department of Electrical and Electronic Engineering,
[2]Lviv Polytechnic National University,
Department of Computer Engineering

CONCURRENT ERROR DETACTION OF DEVICES FOR EXTENDED GALOIS FIELDS ELEMENTS PROCESSING

Abstract. Binary codes of extended Galois fields elements are redundant, some of them never appear at the normal operation of the devices for processing of such field elements. Unused (forbidden) code combinations can be used to organize on-line testing (concurrent error detection) of the specified devices. The appearance of any forbidden combination will be a sign of error. The paper compares the various extended Galois fields with the possibility of on-line testing organization, the fields that best ensure its holding are determined. It is noted that there are no bits for the codes of the Galois field elements that have strictly different values in the allowed and prohibited codes. It is suggested to evaluate the possibility of realizing the testing by the ratio of the number of forbidden combinations to the total number of combinations or to the number of permitted combinations. To achieve the greatest diagnostic effect, it is recommended to use fields with characteristics that are the first prime number greater than degree of 2. In terms of testing price, the best is the GF(3^m) field, for which it is necessary to define only one forbidden code combination, which provides detection of all forbidden codes. When using the Galois GF(d^m) fields under consideration, the minimum coding distance for the codes of each digit of the code is 1. This indicates that it is impossible to detect 100 % of all even single errors in the work of the considered devices in the proposed way. Searching for a logical expression for an error sign is based on the division of groups of consecutive forbidden codes into subgroups. For each subgroup, the bits of its codes are divided into 2 parts, so that the senior bits of each subgroup code remain unchanged, and the younger ones acquire all possible values from 0...0 to 1...1. Then, to the minimized logical error expressions in this subgroup of codes, only the unchanged top bits will enter. Then only the immutable older bits will enter the minimized error expression in this subgroup of codes. The hardware complexity of the proposed method quadratically depends on the number of bits, which encodes one section of the extended Galois fields elements code.

Keywords: extended Galois fields, capacitive complexity, built-in testing

Вступ

Розширені поля Галуа $GF(d^m)$ мають деяку кількість незадіяних кодів своїх елементів. Цю надлишковість можна використати для робочого діагностування пристроїв, що опрацьовують елементи таких полів. Проаналізовано апаратну складність формування ознак помилок на основі використання вказаної надлишковості та запропоновано метод формування ознак помилок під час виконання операцій над елементами скінченних полів Галуа.

1. Аналіз основних публікацій

Сьогодні стандартизовано використання двійкових полів Галуа $GF(2^m)$ для опрацювання електронних цифрових підписів [1, 2]. Крім того, існують стандарти, які визначають використання полів $GF(d^m)$ з характеристикою $d > 3$ (d – просте число), хоча і не заперечують використання трійкових полів з характеристикою $d = 3$ [3]. Для постквантової криптографії зараз аналізують використання поля із характеристикою $d \approx 2^{768}$ [4].

Для прикладних досліджень універсальних алгоритмічних систем обчислень потрібні моделі, які б об'єднали здобутки теорії абстрактних алгоритмів із практикою проектування і розв'язання задач на реальних комп'ютерах. Такою моделлю може бути *SH*-модель (*software-hardware* – програмно-апаратна) алгоритму [5]. У процесах синтезу, аналізі і оптимізації *SH*-моделей запропоновано використовувати п'ять характеристик складності: апаратну, часову, ємнісну, програмну і структурну [6], які пов'язані одна з однією і залежать одна від однієї.

Пристрої, що опрацьовують елементи розширених полів Галуа за показником структурної складності, порівняно у роботах [7–12], апаратної – в [13–15], часової – в [16–18], ємнісної складності – у [19]. Особливості формування ознак, які з'являються при виникненні помилок у роботі пристроїв у різних полях Галуа (робоче діагностування [20]), детально не розглядалися.

2. Постановка завдання

Розглянуто методи робочого діагностування пристроїв опрацювання розширених полів Галуа, а саме, формування ознак, які сповіщають про виникнення помилок у роботі пристроїв. При цьому основна увага приділяється полям $GF(d^m)$ із характеристиками $d > 2$.

3. Представлення елементів полів Галуа у засобах криптографічного захисту інформації

Елементи $\{t^{m-1},...,t^2,t,1\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\{q,q^2,q^{2^2},...,q^{2^{m-1}}\}$ основного поля Галуа утворюють нормальний базис (t і θ – корені полінома p, що утворює поле). Усі інші елементи основного поля Галуа можуть бути представлені як у поліноміальному базисі (у вигляді $a_{m-1}t^{m-1}+...+a_2t^2+a_1t+a_0$), так і у нормальному базисі (у вигляді $a_0q+a_1q^2+a_2q^{2^2}+...+a_{m-1}q^{2^{m-1}}$), де a_i – для двійкового поля Галуа – це двійкові розряди (i = 0, 1, …, m-1) [1]. За будь-яким варіантом елементи розширених полів Галуа $GF(d^m)$ представляються у засобах криптографічного захисту інформації (КЗІ) у вигляді рядка символів $a_{m-1}a_{m-2}...a_1a_0$ (у поліноміальному базисі) або $a_0a_1...a_{m-2}a_{m-1}$ (у нормальному базисі) (рис. 1).

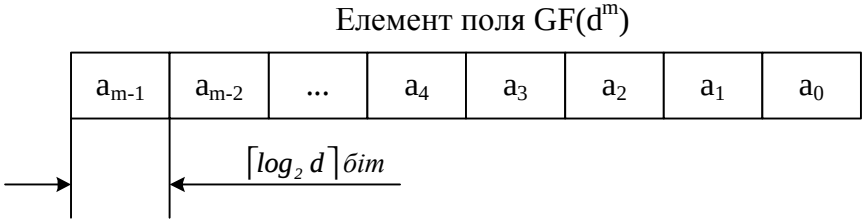


Рис. 1. Представлення елементів полів Галуа

4. Оцінювання тестопридатності представлення елементів розширених полів Галуа

Кожний розряд коду елемента розширеного поля Галуа $GF(d^m)$ представляється $n_b = \lceil \log_2 d \rceil$ бітами, за допомогою яких можна закодувати $d_t = 2^{\lceil \log_2 d \rceil} > d$ різних кодових комбінацій (дозволені коди). При цьому залишається $d_d = d_t - d$ кодових комбінацій, які ніколи не зустрічатимуться при нормальній роботі процесорних вузлів, вузлів пам'яті та каналів передавання даних (заборонені коди). Ці невикористані (заборонені) кодові комбінації можна задіяти для робочого діагностування засобів КЗІ, під час виконання ними їхніх основних функцій, тобто, організувати вбудоване тестування (*concurrent error detection – CED*). Ознакою помилки буде поява будь-якої забороненої комбінації в будь-якому розряді коду будь-якого елемента поля Галуа. Доречно зазначити, що не існує бітів, які мають суворо різні значення в дозволених та заборонених кодах.

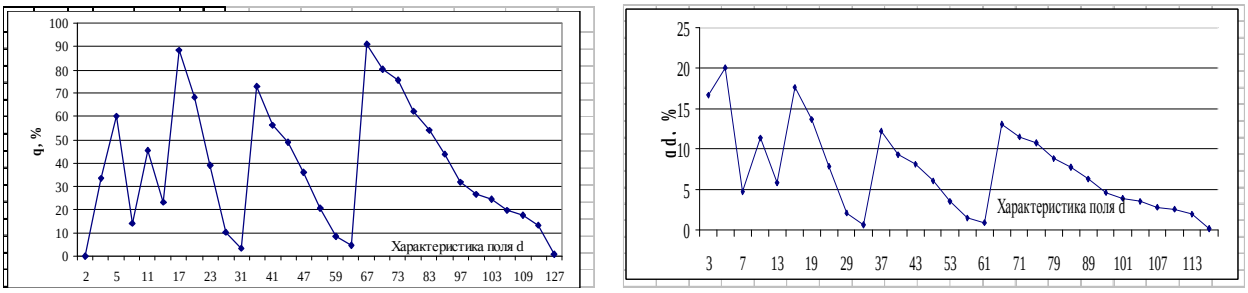
Наприклад, для трійкового поля Галуа $GF(3^m)$ код кожного розряду a_i його елемента (рис. 1) може мати значення, наведені у табл. 1.

Можливість організації діагностування можна оцінити відношенням кількості заборонених комбінацій до загальної кількості комбінацій $q_t = 100*d_d/d_t$ або до кількості дозволених комбінацій $q = 100*d_d/d$. Результати оцінювання можливості організації діагностування при використанні різних розширених полів Галуа наведено у табл. 2 та на рис. 2, *а*. Також можна оцінити зважену можливість діагностування $q_d = q/n_b = 100*d_d/n_b$ (тільки для полів, які мають заборонені значення кодів, рис. 2, *б*), як попереднє значення, ділене на кількість бітів, які необхідно аналізувати для визначення заборонених комбінацій.

Таблиця 1

Вбудоване тестування кодів елементів трійкового поля GF(3m)

ai	Двійковий код a_i, $a_{i1}a_{i0}$	Код	Помилка	Ознака помилки $Error=a_{i1}\&a_{i0}$
0	00	Дозволений	немає	0
1	01	Дозволений	немає	0
2	10	Дозволений	немає	0
3	11	Заборонений	є	1



а *б*

Рис. 2. Якість діагностування полів (а) та зважена якість (б) для GF(d^m), %

Для впровадження діагностування рекомендується використовувати поля з характеристикою d, яка є першим простим числом, більшим за степінь 2, наприклад, $d = 5$. Найменше для робочого діагностування підходять поля з характеристиками d, які є або степенем 2 ($d = 2$), або першим простим числом, меншим за степінь 2, але більшим за 3, наприклад, $d = 127$.

З погляду ціни забезпечення діагностування найкращим є поле $GF(3^m)$ *і*з характеристикою $d = 3$ – для нього необхідно визначати всього одну заборонену кодову комбінацію в кожному з розрядів коду елемента, що забезпечує виявлення усіх заборонених кодів (33 % від усіх можливих кодів). Але для реалізації засобів КЗІ для пост-квантової криптографії розглядаються засоби на основі ізогеній еліптичних кривих, які передбачають використання полів Галуа $GF(d^m)$ із характеристикою $d \approx 2^{768}$.

Важливо підкреслити, що оскільки мінімальна кодова відстань Хеммінга d_H пов'язана з кількістю k помилок, які можна виявити співвідношенням $d_H \geq k + 1$, а при використанні будь-якого поля Галуа $GF(d^m)$ кодова відстань для кодів кожної цифри коду $d_{Hd} = 1$, то кількість помилок k, які можна гарантовано виявити в розглянутих полях, $k \leq 0$. Такий висновок говорить про те, що виявити 100 % усіх навіть поодиноких помилок у роботі розглянутих пристроїв запропонованим способом неможливо. Наприклад, помилка в розряді a_{i0} дозволеного коду 00 (табл. 1) переводить його в інший дозволений код 01 – виявити таку помилку запропонованим методом неможливо. Аналогічна помилка в дозволеному коді 10 переводить його в заборонений код 11, що виявляється запропонованим методом.

Табл. 2 та рис. 2, *а* треба розглядати як оцінку частки помилок, які можна виявляти запропонованим методом.

Також треба розуміти, що проміжні результати обчислень можуть набувати заборонених значень. Наприклад, при додаванні цифр 1 та 2 у трійковому полі ((1 + 2)*mod*3 = 3*mod*3 = 0) проміжна сума набуває забороненого значення 3, яке потім корегується зведенням за модулем 3. У цьому випадку проміжне значення суми, що дорівнює 3, не повинно вважатися помилковим.

5. Формувач ознак помилки опрацювання елементів розширених полів Галуа

Деякі можливі варіанти розміщення дозволених і заборонених кодів серед усіх кодів розрядів елементів полів Галуа зображено на рис. 3. Повний діапазон кодів – це діапазон від $00...0_2$ до $11…1_2$. Дозволені та заборонені коди серед них можуть бути розміщені групами (рис. 3) або вперемішку, розпорошено (такий варіант у цій роботі не розглядається, розглядається тільки розпорошення кодів найбільше на 2 неперервні групи).

Група заборонених кодів може знаходитися наприкінці (рис. 3, *а*), на початку (рис. 3, *б*); в середині (рис. 3, *в*), та по краях (рис. 3, *г*) повного діапазону кодів. Починається *i*-та група заборонених кодів кодом B_i, а закінчується кодом End_i, при виникненні коду із забороненої групи повинна формуватися ознака помилки $Error_i$.

Задача синтезу ознаки помилки $Error_i$ є окремим випадком відомої задачі мінімізації функції багатьох змінних. Розв'язок полегшується тим, що двійкові набори (заборонені коди), які підлягають мінімізації, розташовано послідовно, і їхні коди відрізняються один від одного на +1. Мінімізація в цьому випадку ґрунтується на поділі групи кодів на підгрупи. Для кожної підгрупи розряди її послідовних заборонених кодів діляться на 2 частини так, щоб старші розряди кожного коду з підгрупи залишалися незмінними, а молодші – пробігали всі значення від 0...0 до 1...1. Тоді до мінімізованого логічного виразу ознаки помилки для цієї підгрупи наборів увійдуть тільки незмінні старші розряди [21].

Таблиця 2

Якість контролю полів GF(dm)

d	q_t	q	$log_2 d$	$élog_2 dù$	d_t	d_d	d	q_t	q	$log_2 d$	$élog_2 dù$	d_t	d_d
2	0	0	1	1	2	0	53	17	21	5,7279	6	64	11
3	25	33	1,585	2	4	1	59	8	8	5,8826	6	64	5
5	38	60	2,3219	3	8	3	61	5	5	5,9307	6	64	3
7	13	14	2,8074	3	8	1	67	48	91	6,0661	7	128	61
11	31	45	3,4594	4	16	5	71	45	80	6,1497	7	128	57
13	19	23	3,7004	4	16	3	73	43	75	6,1898	7	128	55
17	47	88	4,0875	5	32	15	79	38	62	6,3038	7	128	49
19	41	68	4,2479	5	32	13	83	35	54	6,375	7	128	45
23	28	39	4,5236	5	32	9	89	30	44	6,4757	7	128	39
29	9	10	4,858	5	32	3	97	24	32	6,5999	7	128	31
31	3	3	4,9542	5	32	1	101	21	27	6,6582	7	128	27
37	42	73	5,2095	6	64	27	103	20	24	6,6865	7	128	25
41	36	56	5,3576	6	64	23	107	16	20	6,7415	7	128	21
43	33	49	5,4263	6	64	21	109	15	17	6,7682	7	128	19
47	27	36	5,5546	6	64	17	113	12	13	6,8202	7	128	15
							127	1	1	6,9887	7	128	1

Наприклад (табл. 3), при мінімізації послідовності 8-бітних кодів $A_0, A_1,..., A_7$ розряди кодів заданих наборів можна розбити на дві групи: незмінну частину – розряди $A_3...A_7$; змінну частину – розряди A_0, A_1, A_2.

Розряди змінної групи перебігають всі можливі значення від 000 до 111. Тому їх можна спростити і записати загальний вираз для всіх заданих у табл. 3 наборів, тобто, для наведеного діапазону кодів $Error_1 = A_7 \overline{A_6} A_5 A_4 A_3$.

У складніших випадках описаний принцип використовується послідовно. Наприклад, для діапазону заборонених кодів 1E3A4...04B8F, які знаходяться всередині повного діапазону кодів, мінімізацію наведено в табл. 4 (показано формування сигналу $Error_1$) та табл. 5 (формування сигналу $Error_2$).

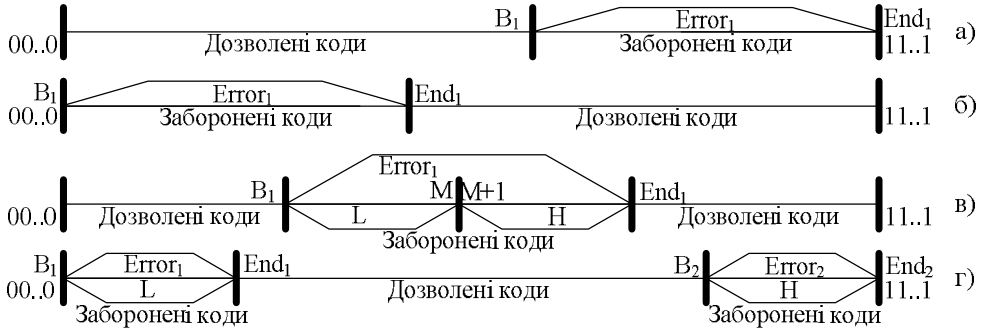


Рис. 3. Дозволені і заборонені коди розрядів елементів полів Галуа GF(d^m)

Таблиця 3

Мінімізація послідовних кодів

Код у 16-ковому коді	Біти коду							
	A_7	A_6	A_5	A_4	A_3	A_2	A_1	A_0
b8	**1**	**0**	**1**	**1**	**1**	*0*	*0*	*0*
b9	**1**	**0**	**1**	**1**	**1**	*0*	*0*	*1*
…								
be	**1**	**0**	**1**	**1**	**1**	*1*	*1*	*0*
bf	**1**	**0**	**1**	**1**	**1**	*1*	*1*	*1*
b8…bf	**1**	**0**	**1**	**1**	**1**	-	-	-

Рядок I_0 (табл. 4) кодує початковий код діапазону – 4B8F. Оскільки його код має в кінці 1, то він у цьому випадку мінімізації не підлягає.

Наступний код – 4B90. Оскільки він закінчується чотирма двійковими нулями, то можна ці чотири розряди виділити в змінну групу і мінімізувати, що і зроблено в рядку I_1.

Останній код, який кодує рядок I_1, дорівнює 4B9F. Він менший за верхню границю діапазону (1E3A4), і тому перевіряється наступний код – 4BA0. Оскільки він закінчується п'ятьма двійковими 0, то можна ці п'ять розрядів виділити у змінну групу і мінімізувати, як це зроблено в рядку I_2.

Останній код, який кодує рядок I_2, дорівнює 4BBF. Він менший за верхню границю діапазону, тому перевіряється наступний код – 4BC0. Оскільки він закінчується шістьма двійковими нулями, то можна ці шість розрядів виділити у змінну групу і мінімізувати, як це зроблено в рядку I_3.

Аналогічні дії виконуються до рядка I_7 включно.

Останній код, який кодує рядок I_8, дорівнює 1FFFF. Він більший за верхню границю діапазону, тому цей рядок є зайвим і з подальшого розгляду вилучається. У результаті отримаємо

$$Error_1 = I_0 \vee I_1 \vee ... \vee I_7 = \overline{A_{16}}\ \overline{A_{15}} A_{14} \overline{A_{13}}\ \overline{A_{12}} A_{11} \overline{A_{10}} A_9 A_8 A_7 \overline{A_6}\ \overline{A_5}\ \overline{A_4} A_3 A_2 A_1 A_0 \vee ... \vee \overline{A_{16}} A_{15}.$$

Ця формула припускає незначні подальші скорочення (використовується формула поглинання $a\bar{b} \vee b = a \vee b$ – зникають закреслені 0 у табл. 4):

$$Error_1 = I_0 \vee I_1 \vee ... \vee I_7 = \overline{A_{16}} A_{14} A_{11} A_9 A_8 A_7 A_3 A_2 A_1 A_0 \vee \overline{A_{16}} A_{14} A_{11} A_9 A_8 A_7 A_4 \vee ... \vee \overline{A_{16}} A_{15}.$$

Подібно створюється таблиця мінімізації старшої частини діапазону заборонених кодів (табл. 5) та формується сигнал $Error_2$.

На відміну від попередньої таблиці, рух відбувається в зворотному напрямі: від верхньої границі до середньої точки (*M* на рис. 3, *в*).

Рядок I_0 кодує кінцевий код діапазону – 1E3A4. Оскільки закінчується 0, то в цьому випадку мінімізації не підлягає. Попередній код – 1E3A3. Оскільки він закінчується двома двійковими одиницями, то можна ці два розряди виділити у змінну групу і мінімізувати, як це зроблено в рядку I_1.

Перший код, який кодує рядок I_1, дорівнює 1E3A0. Він більший за нижню границю діапазону (04B8F), і тому аналізується попередній код – 1E39F. Оскільки він закінчується п'ятьма двійковими 1, то можна ці п'ять розрядів виділити у змінну групу і мінімізувати, як це зроблено у рядку I_2.

Аналогічні дії можна виконувати до рядка I_8 включно.

Таблиця 4

Мінімізація діапазону кодів із довільними границями в напрямку зростання кодів

N	Розряди коду A																Диапазон кодів	
	A16	A15 A14	A13 A12	A11 A10	A9 A8	A7 A6	A5 A4	A3 A2	A1 A0								від	до
I0	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	1	1	04B8F	04B8F
I1	0	0	1	0	0	1	0	1	1	1	0	0	1	–	–	–	–	04B90	04B9F
I2	0	0	1	0	0	1	0	1	1	1	0	1	–	–	–	–	–	04BA0	04BBF
I3	0	0	1	0	0	1	0	1	1	1	1	–	–	–	–	–	–	04BC0	04BFF
I4	0	0	1	0	0	1	1	–	–	–	–	–	–	–	–	–	–	04C00	04FFF
I5	0	0	1	0	1	–	–	–	–	–	–	–	–	–	–	–	–	05000	05FFF
I6	0	0	1	1	–	–	–	–	–	–	–	–	–	–	–	–	–	06000	07FFF
I7	0	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	08000	0FFFF
I8	H	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	10000	1FFFF

Таблиця 5

Мінімізація діапазону кодів із довільними границями в напрямку зменшення кодів

N	Входи A ПЛМ																Диапазон кодів	
	A16	A15 A14	A13 A12	A11 A10	A9 A8	A7 A6	A5	A4	A3	A2	A1	A0					від	до
I0	1	1	1	1	0	0	0	1	1	1	0	1	0	0	1	0	0	1E3A4	1E3A4
I1	1	1	1	1	0	0	0	1	1	1	0	1	0	0	0	–	–	1E3A0	1E3A3
I2	1	1	1	1	0	0	0	1	1	1	0	0	–	–	–	–	–	1E380	1E39F
I3	1	1	1	1	0	0	0	1	1	0	–	–	–	–	–	–	–	1E300	1E37F
I4	1	1	1	1	0	0	0	1	0	–	–	–	–	–	–	–	–	1E200	1E2FF
I5	1	1	1	1	0	0	0	0	–	–	–	–	–	–	–	–	–	1E000	1E1FF
I6	1	1	1	0	–	–	–	–	–	–	–	–	–	–	–	–	–	1C000	1DFFF
I7	1	1	0	–	–	–	–	–	–	–	–	–	–	–	–	–	–	18000	1BFFF
I8	1	0	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	10000	17FFF
I9	0	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	00000	0FFFF

Перший код, який кодує рядок I_9, дорівнює 00000. Він менший за нижню границю діапазону, тому цей рядок є зайвим і з подальшого розгляду вилучається:

$$Error_2 = I_0 \vee I_1 \vee ... \vee I_8 = A_{16}\overline{A_{12}}\,\overline{A_{11}}\,\overline{A_{10}}\,\overline{A_6}\,\overline{A_4}\,\overline{A_3}\,\overline{A_1}\,\overline{A_0} \vee A_{16}\overline{A_{12}}\,\overline{A_{11}}\,\overline{A_{10}}\,\overline{A_6}\,\overline{A_4}\,\overline{A_3}\,\overline{A_2} \vee ... \vee A_{16}\overline{A_{15}}$$

Тут також виконано додаткове спрощення (використовується формула поглинання $a\bar{b} \vee b = a \vee b$ – зникають закреслені 1 у табл. 5).

Таблиці мінімізації для інших варіантів розміщення заборонених кодів (рис. 3) формуються аналогічно.

Можна запропонувати оцінку апаратної складності обчислення сигналу помилки в одному розряді коду елемента розширеного поля Галуа $GF(d^m)$:

- кількість рядків N_r у табл. 4 та табл. 5 приймають приблизно рівною кількості двійкових розрядів $n_b = élog_2dù$ коду, що мінімізується – $N_r \approx n_b = élog_2dù$;
- середня кількість двійкових розрядів N_b у кожному рядку таблиць приймається приблизно рівною $N_b \approx n_b/2$;
- тоді апаратна складність HC_1 визначення ознаки помилки в одному розряді коду елемента розширеного поля Галуа $GF(d^m)$ $HC_1=N_rN_b=n_b^2/2=élog_2dù^{\,2}/2$.

Висновки

Для кращого робочого діагностування пристроїв, що здійснюють опрацювання елементів розширених полів Галуа, рекомендується використовувати поля з характеристикою d, яка є першим простим числом більшим за степінь 2, наприклад, $d = 3$ або $d = 5$. Найменшу якість діагностування дає використання розширених полів із характеристиками d, які є або степенем 2 ($d = 2$), або першим простим числом, меншим за степінь 2, але більшим за 3, наприклад, $d = 127$.

Апаратна складність визначення ознаки помилки в одному розряді коду елемента розширеного поля Галуа $GF(d^m)$ має квадратичну залежність від двійкової довжини коду елемента d.

1. IEEE 1363–2000 (2000). Standard Specifications for Public-Key Cryptography. Copyright © 2000 IEEE. All rights reserved. 2. DSTU 4145–2002. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. ETsP, shcho gruntuietsia na eliptychnykh kryvykh. Formuvannia ta pereviriannia. Kyiv. 2003. 3. DSTU ISO/IEC 15946–1:2015 Informatsiini tekhnolohii. Metody zakhystu. Kryptohrafichni metody, shcho gruntuiutsia na eliptychnykh kryvykh. Chastyna 1. Zahalni polozhennia. 4. De Feo, L. Towards quantum–resistant cryptosystems from supersingular elliptic curve isogenies / L. De Feo, D. Jao, J. Plut // PQCrypto. – 2011.–24 p. 5. Cherkaskyi M. V. SH–model alhorytmu // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" No 433. Vydavnytstvo Natsionalnoho universytetu "Lvivska politekhnika". 2001. S. 127–134. 6. Cherkaskyi M. V., Khusein Khalid Murad. Universalna SH-model // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" No 523 "Kompiuterni systemy ta merezhi". Lviv. Vydavnytstvo Natsionalnoho universytetu "Lvivska politekhnika". 2004. S. 150–154. 7. Hlukhov V. S., Hlukhova O. V. Rezultaty otsiniuvannia strukturnoi skladnosti pomnozhuvachiv elementiv poliv Halua [Tekst] / V. S. Hlukhov, O. V. Hlukhova // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni systemy ta merezhi". – Lviv: – 2013. – Vyp. 773.– S. 27–32. 8. Hlukhov V. S., Trishch H. M. Otsinka strukturnoi skladnosti bahatosektsiinykh pomnozhuvachiv elementiv poliv Halua [Tekst] / V. S. Hlukhov, H. M. Trishch // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni systemy ta merezhi". – Lviv: – 2014. – Vyp. 806. – S. 27–33. 9. Hlukhova, O. V., Lozynskyi, A. Ya., Yaremkevych, R. I., Ihnatovych, A. O. Analitychna otsinka strukturnoi skladnosti pomnozhuvachiv elementiv poliv Halua [Tekst]. / O. V. Hlukhova, A. Ya. Lozynskyi, R. I. Yaremkevych, A. O. Ihnatovych // Materialy V Vseukrainskoi shkoly-seminaru molodykh vchenykh i studentiv. Suchasni kompiuterni informatsiini tekhnolohii. ACIT2015. 22–23 travnia 2015 roku. Ternopil. TNEU. 2015. S. 166–167. 10. R. Elias, M. Rakhma, V. Hlukhov. Strukturna skladnist pomnozhuvachiv elementiv poliv Halua u normalnomu ta polinomialnomu bazysakh. Elektrotekhnichni ta kompiuterni cystemy. – Odesa: – 2017. Vyd-vo Nauka i tekhnika. – No 25 (101). – S. 324–331. 11. Sholohon O.Z. Obchyslennia strukturnoi skladnosti pomnozhuvachiv u polinomialnomu bazysi elementiv poliv Halua GF(2m) [Tekst] / O. Z. Sholohon // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni systemy ta merezhi". – Lviv: – 2014. – Vyp. 806. – S. 284–289. 12. Sholohon Yu. Z. Otsiniuvannia strukturnoi skladnosti pomnozhuvachiv poliv Halua na osnovi elementarnykh peretvoriuvachiv [Tekst] / Yu. Z. Sholohon // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni systemy ta merezhi". – Lviv: – 2014. – Vyp. 806. – S. 290–295. 13. Hlukhov V. S. Porivniannia polinomialnoho ta normalnoho bazysiv predstavlennia elementiv poliv Halua // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni systemy proektuvannia. Teoriia i praktyka". No591, s. 22–27. Lviv, 2007. 14. V. S. Hlukhov. Otsinka aparatnykh vytrat na realizatsiiu bahatorivnevoi kompiuternoi systemy // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Kompiuterni nauky ta informatsiini tekhnolohii" No 629. Lviv, 2008. S. 13–20. 15.

Zholubak, I. M., Hlukhov, V. S. Vyznachennia rozshyrenoho polia Halua GF(dm) z naimenshoiu aparatnoiu skladnistiu pomnozhuvacha [Tekst] / I. M. Zholubak, V. S. Hlukhov // Visnyk Natsionalnoho universytetu "Lvivska politekhnika" "Informatsiini systemy ta merezhi", No 854. Lviv, 2016. S. 63 – 69. 16. Hlukhov V. S., Elias R. M., Rakhma M. K. R. Chasova skladnist oriientovanykh na vykonannia kryptohrafichnykh peretvoren v skladi kiberfizychnykh system pomnozhuvachiv na osnovi modyfikovanykh komirok Hilda. Materialy druhoho naukovoho seminaru Kiber-fizychni systemy: dosiahnennia ta vyklyky, Lviv, Natsionalnyi universytet "Lvivska politekhnika", 21–22 chervnia 2016 r. S. 36–42. 17. R. Elias, M. Rakhma, V. S. Hlukhov. Chasova skladnist pomnozhuvachiv dlia poliv Halua. Elektrotekhnichni ta kompiuterni cystemy. – Odesa: – 2016. Vyd-vo Nauka i tekhnika. – No 22 (98). – S. 323–327. 18. Mohammed Kadhim Rahma, Valeriy S. Hlukhov. Time complexity of multipliers for Galois fields. INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24–26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52–53. 19. R. Elias, V. Hlukhov, M. Rakhma, I. Zholubak. Yemnisna skladnist prystroiv dlia opratsiuvannia elementiv rozshyrenykh poliv Halua. Elektrotekhnichni ta kompiuterni cystemy. – Odesa: – 2018. Vyd-vo Nauka i tekhnika. – No 29 (105) (drukuietsia). 20. Rabochee dyahnostyrovanye bezopasnыkh ynformatsyonno-upravliaiushchykh system / A. B. Drozd, B. C. Kharchenko, S. H Antoshchuk y dr. / Pod red A. B. Drozda, B. C. Kharchenko – Kh. Nats. aэrokosmycheskyi un-t ym. N. E. Zhukovskoho "KhAY", 2012–614 s. 21. Metodychni vkazivky do kursovoi roboty "Aryfmetychni ta lohichni osnovy kompiuternykh tekhnolohii" z dystsypliny "Kompiuterna lohika" bazovoho napriamku 6.050102 "Kompiuterna inzheneriia" / Ukl. V. S. Hlukhov, V. A. Holembo. Lviv: NU"LP", 2014. – 96 s.