УДК 004.382

ЄМНІСНА СКЛАДНІСТЬ ТА ВБУДОВАНИЙ КОНТРОЛЬ ПРИСТРОЇВ ДЛЯ ОПРАЦЮВАННЯ ЕЛЕМЕНТІВ РОЗШИРЕНИХ ПОЛІВ ГАЛУА

Родріг Еліас[1], В. Глухов[2], Мохаммед Рахма[2], І. Жолубак[2]
[1]Ліванський міжнародний університет
[2]Національний університет «Львівська політехніка»

Анотація. *Представлення елементів розширених полів Галуа GF(d^m), коли d>2, мають інформаційну надлишковість. Її можна використати для організації вбудованого контролю операцій над елементами полів. У роботі порівнюються поля GF(d^m) за можливістю організації вбудованого контролю та за ємнісною складністю.*

Ключові слова: *розширені поля Галуа, ємнісна складність, вбудований контроль.*

Вступ

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

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

Порівняння пристроїв, що опрацьовують елементи розширених полів Галуа за показником структурної складності здійснюється у роботах [7], [8], [9], [10], [11], [12], апаратної – в [13], [14], [15], часової – в [16], [17], [18]. Аналіз ємнісної складності та можливості організації вбудованого контролю згаданих пристроїв не проводився.

Тому в роботі саме з цих точок зору аналізуються пристрої, що опрацьовують елементи полів Галуа, розглядаються двійкові поля Галуа GF(2^m), оскільки зараз вони практично використовуються; трійкові поля GF(3^m) – для використання в найближчому майбутньому; інші поля з великими характеристиками GF(p^m), як можлива основа для постквантової криптографії.

1. Представлення елементів полів Галуа у засобах криптографічного захисту інформації

Елементи $\{t^{m-1},...,t^2,t,1\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\{\theta,\theta^2,\theta^{2^2},...,\theta^{2^{m-1}}\}$ 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 $a_0\theta+a_1\theta^2+a_2\theta^{2^2}+...+a_{m-1}\theta^{2^{m-1}}$), де a_i – для двійкового поля Галуа – це двійкові розряди (i = 0, 1, …, m-1) [1]. У будь-якому варіанті елементи розширених полів Галуа *GF(d^m)* представляються у засобах 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).

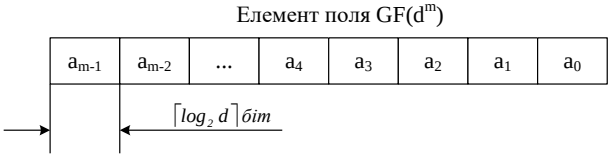

Рис. 1. Представлення елементів полів Галуа

2. Оцінювання ємнісної складності представлення елементів полів Галуа

Для розширених полів Галуа *GF(d^m)* з приблизно однаковим порядком (кількістю елементів поля) об'єм пам'яті, необхідний для збереження кодів елементів (ємнісна складність), буде різним для кожного поля. Якщо взяти поле GF(2^{998}) з порядком 2^{998}, то довжина коду одного елемента буде дорівнювати 998 біт. Для поля

$GF(d^m)$ з порядком $d^m \approx 2^{998}$ довжина коду елемента $LC = m/élog_2dù$. Довжини кодів елементів для різних полів наведено у таблиці 1 та на графіку рис. 2 (Ld – довжина представлення одного розряду коду елемента, K – процент збільшення довжини коду по відношенню до довжини коду елемента поля $GF(2^{998})$, p – просте число, характеристика простого поля Галуа GF(p) таке, що $p \approx 2^{998}$).

Двійкові $GF(2^{998})$ та прості поля Галуа GF(p), а також деякі поля з великими характеристиками мають найменшу довжину коду елементів. Найбільшу довжину коду мають поля з характеристиками 3 та 5, довжини їхніх кодів перевищують довжину коду елементів двійкового поля на 25 - 30 %.

З цієї точки зору найкраще використовувати двійкові та прості поля Галуа, але використання інших полів не приведе до збільшення довжина кодів (ємнісної складності) більше ніж на 30 %.

3. Використання надлишковості кодів елементів розширених полів Галуа для цілей вбудованого контролю

Кожний розряд коду елемента розширеного поля Галуа $GF(d^m)$ представляється $n_b = élog_2dù$ бітами, за допомогою яких можна закодувати $d_t = 2^{élog_2dù} > d$ різних кодових комбінацій. При цьому залишається $d_d = d_t - d$ кодових комбінацій, які ніколи не будуть зустрічатися при нормальній роботі процесорних вузлів, вузлів пам'яті та каналів передачі даних. Ці невикористані (заборонені) кодові комбінації можна задіяти для проведення контролю роботи засобів КЗІ, в ході 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.

Найбільш поширені на сьогоднішній день розширені поля Галуа, що використовуються в засобах КЗІ – двійкові, не мають заборонених значень: кожний розряд a_i коду елемента такого двійкового поля може приймати тільки два значення, 0 або 1. А, наприклад, для трійкового поля Галуа $GF(3^m)$ код кожного розряду a_i його елемента (рис. 1) може мати значення, які містить таблиця 2.

Тому в статті розглядаються не різні методи організації вбудованого контролю, а аналізується можливість організації такого контролю в різних розширених полях Галуа $GF(d^m)$ з різними характеристиками d, але з приблизно однаковим порядком (кількістю елементів поля) d^m.

Таблиця 1

Довжина кодів елементів полів $GF(d^m)$

d	m	Ld	LC	K, %
2	998	1	998	0
3	630	2	1260	26
5	430	3	1290	29
7	356	3	1068	7
11	289	4	1156	16
13	270	4	1080	8
17	245	5	1225	23
19	235	5	1175	18
23	221	5	1105	11
29	206	5	1030	3
31	202	5	1010	1
37	192	6	1152	15
41	187	6	1122	12
43	184	6	1104	11
47	180	6	1080	8
53	175	6	1050	5
59	170	6	1020	2
61	169	6	1014	2
67	165	7	1155	16
71	163	7	1141	14
73	162	7	1134	14
79	159	7	1113	12
83	157	7	1099	10
89	155	7	1085	9
97	152	7	1064	7
101	150	7	1050	5
103	150	7	1050	5
107	149	7	1043	5
109	148	7	1036	4
113	147	7	1029	3
127	143	7	1001	0
251	126	8	1008	1
509	111	9	999	0
###	100	10	1000	0
p	1	998	998	0

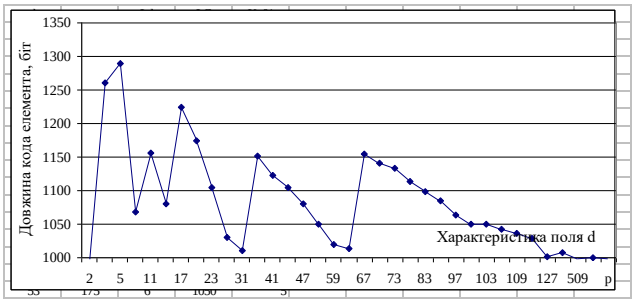

Рис. 2. Довжина кодів елементів полів $GF(d^m)$ в бітах

Придатність розширених полів до вбудованого контролю, що розглядається, залежить від відношення 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 розрахунку цих відношень для різних розширених полів Галуа наведено у таблиці 3 та рис. 3. Також можна оцінити зважену придатність $q_d = q/n_b = 100*d_d/n_b$ (для полів, які мають заборонені значення кодів, рис. 4), як попереднє значення ділене на кількість біт, які необхідно аналізувати для визначення заборонених комбінацій.

Таблиця 2

Вбудоване тестування кодів елементів трійкового поля GF(3^m)

a_i	Двійковий код a_i, $a_{i1}a_{i0}$	Код	Помил-ка	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

Для збільшення рівня вбудованого контролю рекомендується використовувати поля з характеристикою d, яка є першим простим числом більшим за степінь 2, наприклад, d = 5. Найменший рівень вбудованого контролю дає використання полів з характеристиками d, які є або степенем 2 (d = 2), або є першим числом меншим за степінь 2, але більшим за 3, наприклад, d = 127.

З точки зору ціни вбудованого контролю, найкращим є поле з характеристикою d = 3 (розширене трійкове поле Галуа GF(3^m) - необхідно визначати всього одну заборонену кодову комбінацію в кожному з розрядів коду елемента і це забезпечує охоплення вбудованим контролем на рівні 33 %.

Важливо підкреслити, що оскільки мінімальна кодова відстань Хеммінга d_H зв'язана з кількістю k помилок, які можна виявити, співвідношенням $d_H \geq k + 1$, а при використанні будь-якого поля Галуа $GF(p^m)$ кодова відстань для кодів кожної цифри коду $d_{Hd} = 1$, то кількість помилок, які можна виявити в розглянутих полях, $0 \geq k$.

Такий висновок говорить про те, що виявити 100 % усіх навіть поодиноких помилок неможливо. Таблицю 3 та рис. 3 треба розглядати як оцінку частки помилок, які можна виявляти запропонованим методом.

Запропонований метод дозволяє частково визначати константні помилки, які можуть виникати під час роботи засобів КЗІ. Наприклад, константна помилка в розряді a_{i0} (постійне закорочення на 1) дозволеного коду 00 (таблиця 2) 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. Також можна виявляти і динамічні помилки (міжрозрядні закорочення), якщо у конфліктних ситуаціях (закорочення джерела логічного 0 та джерела логічної 1) спотворений сигнал буде сприйматися приймачем як 1. Наприклад, закорочення розрядів a_{i1} та a_{i0} в цій ситуації приведе до перетворення їхніх коректних комбінацій 01 та 10 у заборонену комбінацію 11, яка буде виявлена запропонованим методом.

Таблиця 3

Рівень вбудованого контролю полів GF(d^m)

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

Також треба розуміти, що проміжні результати обчислень можуть набувати заборонених значень. Наприклад, при додаванні

цифр 1 та 2 у трійковому полі ((1 + 2)mod3 = 3mod3 = 0) проміжна сума набуває забороненого значення 3, яке потім коректується зведенням за модулем 3. У даному випадку проміжне значення суми, рівне 3, не повинно вважатися помилковим.

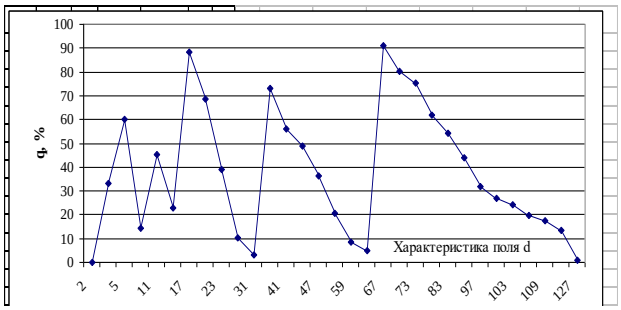

Рис. 3. Рівень вбудованого контролю полів GF(d^m), %

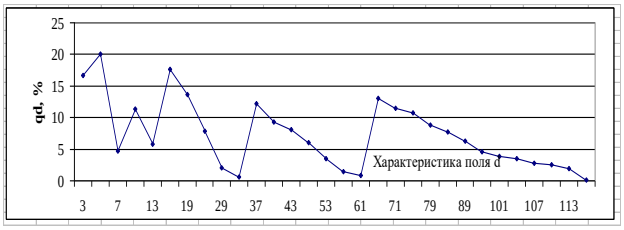

Рис. 4. Зважений рівень вбудованого контролю полів GF(d^m), %

Висновки

У роботі показано що розширені двійкові та прості поля Галуа мають найменшу довжину кодів елементів поля (найменшу ємнісну складність), але використання інших розширених полів Галуа не приведе до збільшення довжина кодів елементів (ємнісної складності) більше ніж на 30 %.

Для більш ефективного вбудованого контролю 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 ефективність вбудованого контролю дає використання полів з характеристиками d, які є або степенем 2 ($d = 2$), або є першим числом меншим за степінь 2, але більшим за 3, наприклад, $d = 127$.

З точки зору ціни вбудованого контролю, найкращим є поле з характеристикою $d = 3$ (розширене трійкове поле Галуа $GF(3^m)$).

Використання надлишковості, яку мають розширені поля Галуа з характеристиками $d > 2$, не забезпечує виявлення усіх помилок, які можуть виникати під час опрацювання елементів таких полів.

Список використаної літератури

1. IEEE 1363-2000 (2000). Standard Specifications for Public-Key Cryptography [Text]. Copyright © 2000 IEEE. All rights reserved.

2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. ЕЦП, що ґрунтується на еліптичних кривих. Формування та перевіряння [Текст]. Київ. 2003.

3. ДСТУ ISO/IEC 15946-1:2015 Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Загальні положення [Текст].

4. De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [Text] / L. De Feo, D. Jao, J. Plut // PQCrypto. – 2011. – 24 p.

5. Черкаський, М. В. SH-модель алгоритму [Текст] // Вісник Національного університету "Львівська політехніка" № 433. Видавництво Національного університету «Львівська політехніка». 2001. С.127–134.

6. Черкаський, М. В., Хусейн Халід Мурад. Універсальна SH-модель [Текст] // Вісник Національного університету "Львівська політехніка" № 523 «Комп'ютерні системи та мережі». Львів. Видавництво Національного університету «Львівська політехніка». 2004. С.150–154.

7. Глухов, В. С., Глухова, О. В. Результати оцінювання структурної складності помножувачів елементів полів Галуа [Текст] / В. С. Глухов, О. В. Глухова // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: - 2013. - Вип. 773. - С. 27–32.

8. Глухов, В. С., Тріщ, Г. М. Оцінка структурної складності багатосекційних помножувачів елементів полів Галуа [Текст] / В. С. Глухов, Г. М. Тріщ // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: - 2014. - Вип. 806. - С. 27–33.

9. Глухова, О. В., Лозинський, А. Я., Яремкевич, Р. І., Ігнатович, А. О. Аналітична оцінка структурної складності помножувачів елементів полів Галуа [Текст]. / О. В. Глухова, А. Я. Лозинський, Р. І. Яремкевич, А. О. Ігнатович // Матеріали V Всеукраїнської школи-семінару молодих вчених і студентів. Сучасні комп'ютерні інформаційні технології. ACIT'2015. 22-23 травня 2015 року. Тернопіль. ТНЕУ. 2015. С. 166–167.

10. Еліас, Р., Рахма, М., Глухов, В. Структурна складність помножувачів елементів

полів Галуа у нормальному та поліноміальному базисах [Текст]. Електротехнічні та комп'ютерні системи. – Одеса: – 2017. Вид-во Наука і техніка. - № 25 (101). – С. 324–331.

11. Шологон, О. З. Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа $GF(2^m)$ [Текст] / О. З. Шологон // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". - Львів: - 2014. - Вип. 806. - С. 284–289.

12. Шологон, Ю. З. Оцінювання структурної складності помножувачів полів Галуа на основі елементарних перетворювачів [Текст] / Ю. З. Шологон // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". - Львів: - 2014. - Вип. 806. - С. 290–295.

13. Глухов, В. С. Порівняння поліноміального та нормального базисів представлення елементів полів Галуа [Текст] // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". №591, с.22–27. Львів, 2007.

14. Глухов, В. С. Оцінка апаратних витрат на реалізацію багаторівневої комп'ютерної системи [Текст] // Вісник Національного університету «Львівська політехніка» «Комп'ютерні науки та інформаційні технології» № 629. Львів, 2008. С.13–20.

15. Жолубак, І. М., Глухов, В. С. Визначення розширеного поля Галуа $GF(d^m)$ з найменшою апаратною складністю помножувача [Текст]. / І. М. Жолубак, В. С. Глухов // Вісник Національного університету «Львівська політехніка» "Інформаційні системи та мережі", № 854. Львів, 2016. С. 63–69.

16. Глухов, В. С., Еліас, Р. М., Рахма, М. К. Р. Часова складність орієнтованих на виконання криптографічних перетворень в складі кіберфізичних систем помножувачів на основі модифікованих комірок Гілда [Текст]. Матеріали другого наукового семінару Кібер-фізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р. С. 36–42.

17. Еліас, Р., Рахма, М., Глухов, В. С. Часова складність помножувачів для полів Галуа [Текст]. Електротехнічні та комп'ютерні системи. – Одеса: – 2016. Вид-во Наука і техніка. – № 22 (98). – С. 323–327.

18. Rahma, M. K., Hlukhov, V. S. Time complexity of multipliers for Galois fields [Text]. INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24-26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52–53.

References

1. IEEE 1363-2000 (2000). Standard Specifications for Public-Key Cryptography [Text]. Copyright © 2000 IEEE. All rights reserved.

2. DSTU 4145-2002 (2002), Information Technology. Cryptographic Techniques. Digital Signatures Based on Elliptic Curves. Generation and Verification [Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Tsyfrovyy pidpys, shcho gruntuyet'sya na eliptychnykh kryvykh. Formuvannya ta pereviryannya], *Derzhavnyy komitet Ukrayiny z pytan' tekhnichnoho rehulyuvannya ta spozhyvchoyi polityky*, Kiyv, Ukraine, 2003 (In Ukrainian).

3. DSTU ISO/IEC 15946-1:2015 Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General [DSTU ISO/IEC 15946-1:2015 Informatsiini tekhnolohii. Metody zakhystu. Kryptohrafichni metody, shcho gruntuiutsia na eliptychnykh kryvykh. Chastyna 1. Zahalni polozhennia], Kiyv, Ukraine, 2016 (In Ukrainian).

4. De Feo, L. (2011), Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. PQCrypto. – 24 p.

5. Cherkaskyi, M. V. (2001), SH-model of the algorithm [SH-model alhorytmu] // *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 433, pp. 127–134 (In Ukrainian).

6. Cherkaskyi, M. V., Khusein Khalid Murad (2004). Universal SH-model [Universalna SH-model] // *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, vol. 523, pp. 150–154 (In Ukrainian).

7. Hlukhov, V. S., Hlukhova, O. V. (2013), Structural Complexity of Galois Field Elements Multipliers Evaluation Results [Rezul'taty otsinky strukturnoyi skladnosti pomnozhuvachiv elementiv poliv Halua], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 773, pp. 27–32 (In Ukrainian).

8. Hlukhov, V. S., Trishch, H. M. (2014), Evaluation of structural complexity of multisection multiplier for Galois field elements [Otsinka strukturnoyi skladnosti bahatosektsiynykh pomnozhuvachiv elementiv poliv Halua], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 27–33 (In Ukrainian).

9. Hlukhova, O. V., Lozynskyi, A. Ya., Yaremkevych, R. I., Ihnatovych, A. O. (2015),

Analytical evaluation of Galois field elements multipliers structural complexity [Analitychna otsinka strukturnoi skladnosti pomnozhuvachiv elementiv poliv Halua], *Materialy V Vseukrainskoi shkoly-seminaru molodykh vchenykh i studentiv. Suchasni kompiuterni informatsiini tekhnolohii. ACIT'2015*, 22-23 may 2015 year. Ternopil. Ukraine. TNEU. Pp. 166–167 (In Ukrainian).

10. Elias, R., Rakhma, M., Hlukhov, V. (2017), Structural complexity of multipliers for Calois fields elements in normal and polynomial bases [Strukturna skladnist pomnozhuvachiv elementiv poliv Halua u normalnomu ta polinomialnomu bazysakh]. *Elektrotehnicheskie i kompyuternyie sistemy*, Odessa, Ukraine, № 25 (101), pp. 324–331 (In Ukrainian).

11. Sholohon, O. Z. (2014), Structural Complexity of Galois Field GF(2^m) Elements Multipliers in Polynomial Basis Calculation [Obchyslennya strukturnoyi skladnosti pomnozhuvachiv u polinomial'nomu bazysi elementiv poliv Halua GF(2^m)], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 284–289 (In Ukrainian).

12. Sholohon, Yu. Z. (2014), Based on Elementary Transducers Structural Complexity of Galois Field Multipliers Evaluation [Otsinyuvannya strukturnoyi skladnosti pomnozhuvachiv poliv Halua na osnovi elementarnykh peretvoryuvachiv], *Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi"*, Lviv, Ukraine, vol. 806, pp. 290–295 (In Ukrainian).

13. Hlukhov, V. S. (2007), Comparison of polynomial and normal bases of Galois fields elements presentation [Porivnyannya polinomial"noho ta normal"noho bazysiv predstavlennya elementiv poliv Halua, *Visnyk Natsionalnoho universytetu «Lvivska politekhnika» "Komp'yuterni systemy proektuvannya. Teoriya i praktyka"*, Lviv, Ukraine, vol. 591, pp. 22–27 (In Ukrainian).

14. Hlukhov, V. S. (2008), Estimation of hardware costs for implementation of multilevel computer system [Otsinka aparatnykh vytrat na realizatsiiu bahatorivnevoi kompiuternoi systemy] // *Visnyk Natsionalnoho universytetu «Lvivska politekhnika»* "Kompiuterni nauky ta informatsiini tekhnolohii" Lviv, Ukraine, vol. 629, pp. 13–20 (In Ukrainian).

15. Zholubak, I. M., Hlukhov, V. S. (2016), Definition of the extended Galois field GF(d^m) with multiplier minimal hardware complexity [Vyznachennia rozshyrenoho polia Halua GF(d^m) z naimenshoiu aparatnoiu skladnistiu pomnozhuvacha], *Visnyk Natsionalnoho universytetu «Lvivska politekhnika» "Informatsiini systemy ta merezhi"*, vol. 854. Lviv, Ukraine, Pp. 63–69 (In Ukrainian).

16. Hlukhov, V., Elias, R., Rahma, M. (2016), The time complexity of based on modified Guild cells and oriented on cryptographic transformations in cyberphysical systems multipliers [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*, pp. 36–42 (In Ukrainian).

17. Elias, R., Rahma, M., Hlukhov, V. (2016), Multipliers for Galois fields time complexity [Chasova skladnist' pomnozhuvachiv dlya poliv Halua], *Elektrotehnicheskie i kompyuternyie sistemy*, Odessa, Ukraine, № 22 (98), pp. 323–327 (In Ukrainian).

18. Rahma, M. K., Hlukhov, V. S. (2016), Time complexity of multipliers for Galois fields. INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24-26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52–53.

CAPACITY COMPLEXITY AND EMBEDDED ERROR DETECTION OF DEVICES FOR EXTENDED GALOIS FIELDS ELEMENTS PROCESSING

Rodrigue Elias[1], V. Hlukhov[2], Mohammed Rahma[2], I. Zholubak[2]
[1]Lebanese International University
[2]Lviv Polytechnic National University

Abstract. *For extended Galois fields GF(d^m) of about the same order (number of field elements) the amount of memory required to store elements codes (capacitive complexity) will be different for each field. Each digit of extended Galois field GF(d^m) element code is represented by $n_b = \acute{e}log_2 d\grave{u}$ bits, by which you can encode $d_t = 2^{\acute{e}log_2 d\grave{u}} > d$ of different code combinations. At the same time, $d_d = d_t - d$ code combinations remain, which will never be encountered in the normal operation of processor and memory units and data*

channels. These unused (forbidden) code combinations can be used to control the work of these devices in the course of performing their basic functions, that is, to organize in-built testing, so called concurrent error detection (CED). Appearance of any forbidden combination in any Galois field element code digit will be the sign of error. In this paper, various extended Galois fields with approximately the same number of elements are compared by the capacitive complexity and concurrent error detection ability of the devices for such fields elements processing.

To date, the use of Galois GF(2^m) binary fields has been standardized for the processing of digital signatures. In addition, there are standards that determine the use of the fields GF(p^m) with the characteristic p > 3 (p is a prime number), although they do not deny the use of ternary fields with the characteristic p = 3. Fields with characteristic $p \approx 2^{768}$ are now being analyzed for use in post-quantum cryptography. For applied research of universal algorithmic computing systems models are needed that combine the achievements of the theory of abstract algorithms with the practice of designing and solving problems on real computers. The SH-model of the algorithm (software-hardware model) can be one. In the processes of synthesis, analysis and optimization of SH-models, it is proposed to use five complexity characteristics: hardware, time, capacitive, programmatic and structural ones, which are connected with each other and depend on each other.

Comparison of devices that process elements of extended Galois fields by the indicator of structural, hardware and time complexities was carried out in earlier works. Analysis of the capacity complexity and concurrent error detection ability of mentioned devices was not carried out.

Therefore, in the work in terms of capacitive complexity and concurrent error detection ability of devices that process Galois fields elements the next extended fields are considered: binary Galois field GF(2^m), since they are now practically used; ternary fields GF(3^m) - for use in the near future; other fields with high characteristics GF(p^m) which are supposed to be involved in post-quantum cryptography.

It is shown in this paper that extended binary and prime Galois fields have the smallest length of elements codes (the smallest capacitive complexity), but the use of other extended Galois fields will not increase the length of the elements codes (capacitive complexity) by more than 30%. In order to increase the concurrent error detection ability of devices that process the extended Galois fields elements, it is recommended to use fields with characteristic d, which is the first prime number greater than power of 2, for example d = 3 or d = 5. Fields with characteristics d, which are either of power of 2 (d = 2), or are the first number smaller than the power of 2, but greater than 3, for example, d = 127, have the least concurrent error detection ability. From the standpoint of concurrent error detection cost, the field with a characteristic d = 3 (the extended ternary Galois GF(3m)) is the best. The redundancy of the extended Galois fields with characteristics d > 2 does not guarantee the detection of all errors that may occur when processing elements of such fields.

Keywords: *extended Galois fields, capacitive complexity, concurrent error detection*

ЕМКОСТНАЯ СЛОЖНОСТЬ И ВСТРОЕННЫЙ КОНТРОЛЬ УСТРОЙСТВ ДЛЯ ОБРАБОТКИ ЭЛЕМЕНТОВ РАСШИРЕННЫХ ПОЛЕЙ ГАЛУА

Родриг Элиас[1], В. Глухов[2], Мохаммед Рахма[2], И. Жолубак[2]
[1]Ливанский международный университет
[2]Национальный университет «Львовская политехника»

Аннотация. *Представления элементов расширенных полей Галуа GF(d^m), когда d>2, имеют информационную избыточность. Ее можно использовать для организации встроенного контроля операций над элементами полей. В работе сравниваются поля GF(d^m) по возможности организации встроенного контроля и по емкостной сложности.*

Ключевые слова: *расширенные поля Галуа, емкостная сложность, встроенный контроль.*

Отримано 29.10.2018

Еліас Родріг Митрі, кандидат технічних наук, інструктор кафедри електротехніки та електронної інженерії Ліванського міжнародного університету, Школа інженерії, Блок G, Ліванський міжнародний університет, P.O. Box: 146404, Бейрут, Ліван, E-mail: rodrigue.elias@liu.edu.lb, м/т.: 961.3.492949

Elias Rodrigue Metri, PhD, an instructor at the School of Engineering at the Lebanese International University, School of Engineering, Block G, Lebanese International University, P.O. Box: 146404 Beirut, Lebanon
E-mail: rodrigue.elias@liu.edu.lb, Tel.: 961.3.492949
ORCID ID: 0000-0003-4506-0368

Глухов Валерій Сергійович, доктор технічних наук, професор, професор кафедри електронних обчислювальних машин Національного університету «Львівська політехніка», вул. С. Бандери, 12, Львів, Україна, E-mail: glukhov@polynet.lviv.ua , м/т.: +38-063-75-72-330.

Valeriy Hlukhov, Dr. of Science, Professor, Professor of the Department of Computer Engineering, Lviv Polytechnic National University, S. Bandera Str., 12, Lviv, Ukraine, E-mail: glukhov@polynet.lviv.ua, м/т.: +38-063-75-72-330.
ORCID ID:0000-0002-0542-7447

Рахма Мохаммед Кадім, аспірант кафедри електронних обчислювальних машин Національного університету «Львівська політехніка», вул. С. Бандери, 12, Львов, Україна, E-mail: muhamed_kadhem@yahoo.com , +38-093-19-62-350

Rahma Mohammed Kadhim, PhD student of the Department of Computer Engineering, Lviv Polytechnic National University, S. Bandera Str., 12, Lviv, Ukraine, E-mail: muhamed_kadhem@yahoo.com, +38-093-19-62-350
ORCID ID: 0000-0002-8377-1833

Жолубак Иван Михайлович, асистент кафедри електронних обчислювальних машин Національного університету «Львівська політехніка», вул. С. Бандери, 12, Львів, Україна, E-mail: ivanzholubak7@ukr.net, +380 63 204 3548

Ivan Zholubak, assistant of the Department of Computer Engineering, Lviv Polytechnic National University, S. Bandera Str., 12, Lviv, Ukraine, E-mail: ivanzholubak7@ukr.net, +380 63 204 3548
ORCID ID: 0000-0001-8871-7222