УДК 004.382

І. М. Жолубак, В. С. Глухов
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

РЕАЛІЗАЦІЯ У ПЛІС ПОМНОЖУВАЧІВ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА ВИСОКИХ ПОРЯДКІВ

Розглянуто реалізацію матричних помножувачів полів Галуа з основами 2, 5, 3, 7, 13 та вищими основами на ПЛІС фірмиXilinx – Spartan-6 та Altera – Cyclone-5. Показано, що найменшими апаратні затрати будуть у помножувачів полів Галуа з основою 2. Для реалізації помножувачів полів Галуа різних основ розроблено програму для автоматизованого синтезу VHDL коду помножувачів.

Ключові слова: поля Галуа GF (d^m), помножувач, модифікована комірка Гілда, LUT, генератор ядер.

I. Zholubak, V. Hlukhov
Lviv Polytechnic National University,
Computer Engineering Department

MULTIPLIER REALIZATION IN FPGA OF THE HIGH LEVEL GALOIS FIELDS

In this paper, the implementation of matrix multipliers of the Galois fields with basics 2, 3, 5, 7, 13 and the analysis of the implementation of multipliers with a higher basis on the FPGA Xilinx Spartan-6 and Altera – Cyclone-5 is considered. It is shown that the smallest hardware costs will be in multiples of Galois fields with a base 2. For the implementation of the Guild cells with a large foundation, the core generator of the modified Guild cells was implemented.

Key words: Galois fields GF (d^m), multiplier, modified Guild cell, LUT, nucleus generator.

Вступ

Сьогодні набули актуальності криптографічні методи захисту інформації на основі використання ПЛІС та криптографічних протоколів, побудованих на операціях множення у полях Галуа GF (n^m). Матричні помножувачі полів Галуа GF (n^m) характеризуються великими апаратними витратами, а тому стає доцільним пошук найкращого методу їхньої реалізації. У роботі здійснено порівняння апаратних затрат помножувачів полів Галуа GF (n^m) за результатами їхньої практичної реалізації у ПЛІС.

Аналіз літературних джерел

У [4] для зменшення апаратної складності помножувача елементів полів Галуа, основним елементом якого є помножувальна матриця, запропоновано підхід, який полягає у заміні помножувальної матриці розміром m×m на перемішувач та впорядковану модифіковану помножувальну матрицю меншого розміру. Зменшення, внаслідок цього, структурної [7] та апаратної складності призведе до збільшення часової складності множення [5]. Для визначення можливостей реалізації помножувача на ПЛІС необхідна точніша оцінка апаратної та часової

складності з урахуванням особливостей топології ПЛІС. Метою роботи є оцінка апаратних затрат на створення помножувальної матриці [6] помножувача елементів полів Галуа у поліноміальному базисі та вибору поля, у якому апаратні затрати будуть найменшими. Під час виконання цієї роботи на основі запропонованої у [1] та [2] моделі помножувача здійснено його імплементацію та перевірку отриманих теоретично у [1] та [2] результатів апаратної складності.

ПЛІС фірми Xilinx [8] складаються з логічних блоків – CLB (Configurable Logic Block). Елемент CLB містить два елементи SLICE, кожен елемент складається з чотирьох шестивхідних LUT і восьми елементів зберігання. SLICE (0) – елемент у нижній частині CLB, SLICE (1) – елемент у верхній частині CLB. Ці два елементи не мають прямих зв'язків один з одним.

Таблиці перекодування реалізуються як таблиці істинності (LUT). В LUT є шість незалежних входів (А входи – А1 до А6) і два незалежні виходи (О5 і О6). Функціональні генератори можуть реалізувати за допомогою однієї LUT будь-яку довільно визначену логічну функцію, яка залежить від шести змінних; дві довільно визначені п'ятивходові логічні функції, якщо ці дві функції мають спільні входи; дві довільно визначені логічні функції з трьома та двома входами.

Мета роботи

Метою роботи є практичне порівняння апаратних витрат для створення помножувачів елементів полів Галуа з різними основами, але приблизно однаковою кількістю елементів поля, на ПЛІС. Коди елементів полів Галуа подаються в поліноміальному базисі.

Реалізація на ПЛІС

Розвиток зв'язків між людьми, науково-технічного прогресу та економіки привів до появи нової сфери взаємовідносин між людьми, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні й некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках. В електронному документі відомості, зафіксовані за допомогою електронних даних, мають містити обов'язкові реквізити документа, найголовнішим з яких є електронний підпис, в іншому випадку це документ в електронному вигляді. Тобто без електронного підпису за певних вимог документ не має юридичної сили і не може бути електронним документом.

Одним із методів захисту електронної інформації є електронний цифровий підпис (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документа, його реквізитів і факту підписання конкретною особою. Документи можуть бути засвідчені електронним цифровим підписом і передані до місця призначення протягом декількох секунд, адже електронний документ передається за допомогою швидкісних телекомунікаційних систем, однією з яких є, наприклад, Інтернет. За таких умов усі учасники обміну електронними документами незалежно від відстані мають однакові можливості в електронному інформаційному обміні.

Електронний цифровий підпис реалізується виконанням операцій у полях Галуа. Для виконання операції множення у полях Галуа можна застосовувати матричний помножувач. Він має певні переваги та недоліки. Серед недоліків – велика апаратна та структурна складності, серед переваг – висока швидкодія за апаратної реалізації помножувача.

Матричні помножувачі виконують операцію множення не традиційно послідовними зсувами та додаваннями, а паралельно. Схема виконання операції множення відповідає звичайному "множенню стовпчиком". В матриці відбувається порозрядне множення розрядів та підсумування проміжних результатів. Для операції множення та підсумування проміжних результатів використовують модифіковані комірки Гілда (КГ).

Модифіковані КГ для полів Галуа GF (d^m) мають 3p входи та p виходів, розрядністю $p = \lceil \log_2 m \rceil$ біт кожний. Модифіковану КГ можна розглядати за двома варіантами:

1) вважати комірку Гілда “чорною скринькою” – повністю цілісним елементом, в якому несуттєвою є внутрішня структура, а до уваги береться тільки кількість входів та виходів;

2) з уточненням внутрішньої структури (комірка Гілда складається з помножувача та суматора).

У першому варіанті кількість LUT, які використовуються для реалізації однієї модифікованої КГ – $k_{gd} = (|\,2^{(p-5)} - 1|) * k$, де $p = 3 * \lceil \log_2 d \rceil$, коли d > 2 та $p = 4 * \lceil \log_2 d \rceil$, коли d = 2, $k = \lceil \log_2 d \rceil$. Звідси випливає що $k_{gd} = (|\,2^{3*\lceil \log_2 d \rceil - 5} - 1|) * \lceil \log_2 d \rceil$, якщо d > 2. Отже:

$$k_{g(d>2)} = (|\,2^{3*\lceil \log_2 d \rceil - 5} - 1|) * \lceil \log_2 d \rceil \quad (1)$$

$$k_{g(d=2)} = (|\,2^{4*\lceil \log_2 d \rceil - 5} - 1|) * \lceil \log_2 d \rceil \quad (2)$$

Для реалізації помножувача в полях Галуа з основою d GF (d^m) потрібно – $k_{kd} = 2m^2 - m$ модифікованих КГ та додатково $(m-1)$ LUT для знаходження коефіцієнта, на який потрібно перемножити незвідний поліном. Апаратними витратами на реалізацію елемента f, який формує цей коефіцієнт, можна в цьому випадку знехтувати, оскільки вони малі порівняно з витратами на реалізацію самих комірок Гілда.

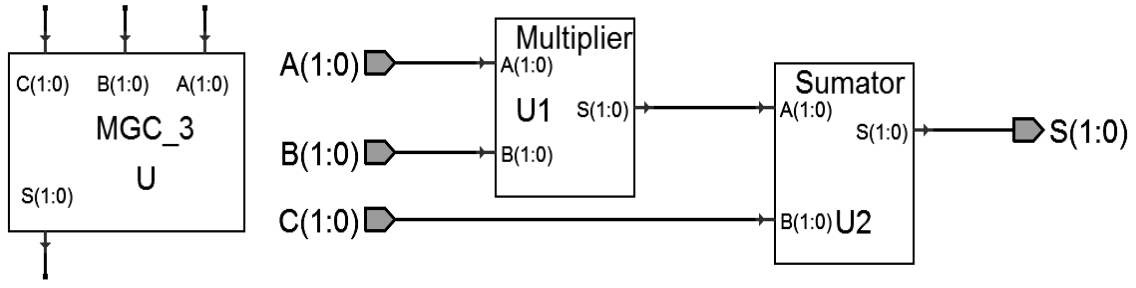
Апаратні витрати у разі реалізації модифікованої КГ за другим варіантом, тобто як сукупності помножувача та суматора, обчислюють за формулою: $k_{gd} = (2^{2*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2$, коли d > 2 та $k_{gd} = (2^{2*\lceil \log_2 d \rceil - 6}) * \lceil \log_2 d \rceil * 2$, коли d = 2. Отже:

$$k_{g(d>2)} = (2^{2*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2 \quad (3)$$

$$k_{g(d=2)} = (2^{2*\lceil \log_2 d \rceil - 6}) * \lceil \log_2 d \rceil * 2 \quad (4)$$

У полях Галуа GF (d^m) для реалізації помножувача потрібно – $2m^2 - m$ КГ. Витратами на реалізацію елемента f нехтуємо, оскільки вони малі, порівняно з витратами на реалізацію самого помножувача.

На рис. 1 подано внутрішню структуру модифікованої КГ у разі реалізації як: а) “чорної скриньки”; та б) з уточненням внутрішньої структури помножувача GF (3^4).



а *б*

Рис. 1. Реалізація модифікованої КГ для полів Галуа GF (3^4):
а – “чорна скринька”; б – з уточненням внутрішньої структури

У першому варіанті формується одна функція, що залежить від шести змінних, яка виконує множення за модулем 3 та додавання за модулем 3, у другому – дві функції, які залежать від чотирьох змінних, перша з яких виконує множення за модулем 3, а друга – додавання за модулем 3.

Проекти створено в середовищі Active HDL 9.1, симуляцію здійснено у середовищі Xilinx ISE для Spartan 6, та у Quartus для Cyclone 5.

Значення апаратних витрат та часових затримок на реалізацію помнжувачів GF (2^{15}), GF (3^9), GF (5^6), GF (7^5), GF (13^4), які усі мають схеми, аналогічні рис. 2, наведено на графіках (рис. 3, 4) та у табл. 1 та 2.

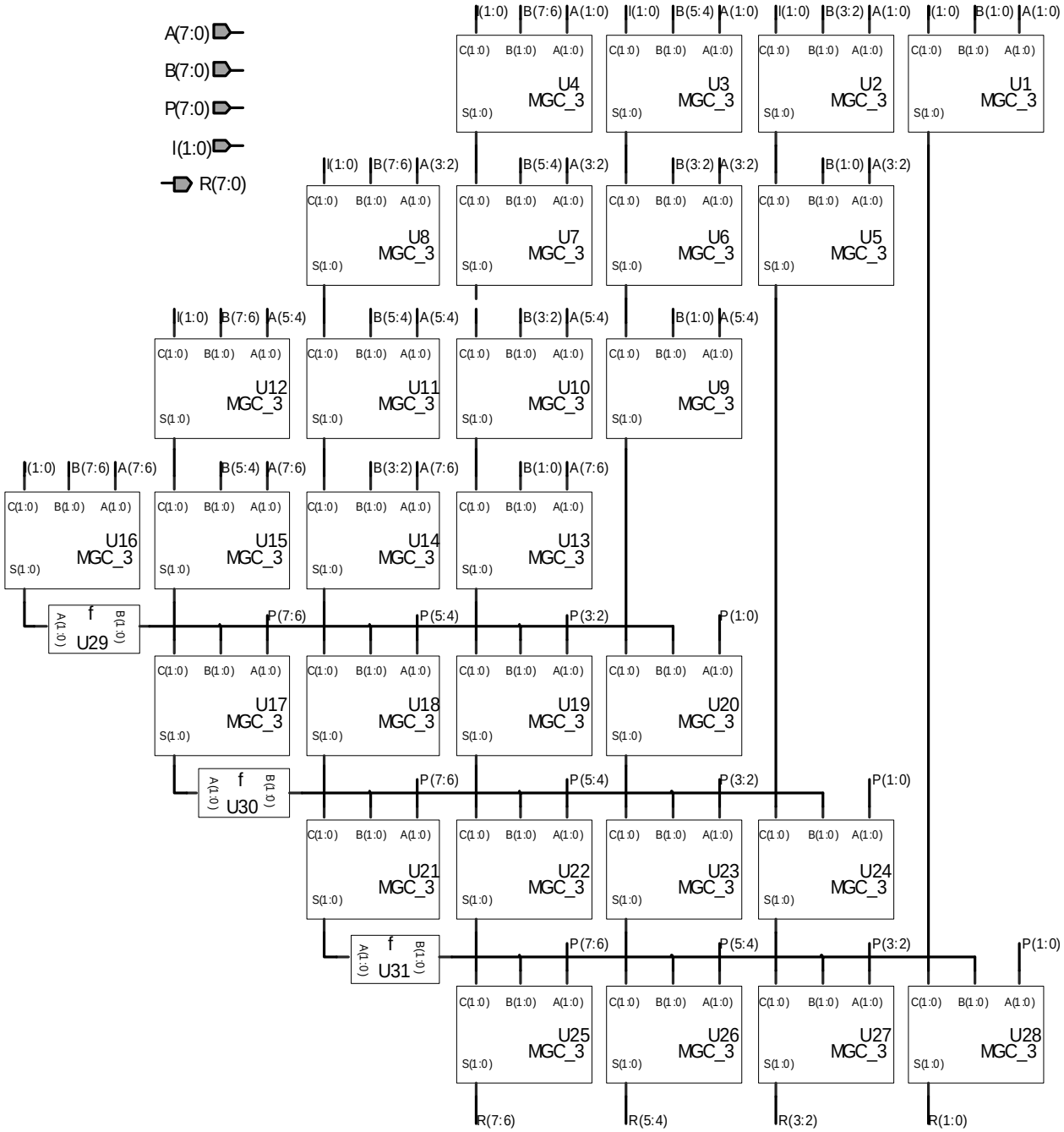


Рис. 2. Схема помножувача полів Галуа GF (3^4)

З графіків (рис. 3, 4) видно, що найменші апаратні затрати має помножувач для елементів поля GF (2^{15}). Найменші часові затримки теж у помножувачів у полях GF (2^{15}). Також зазначимо, що GF (3^9) GF (7^5) мають хороші показники щодо апаратних затрат та швидкодії, які є трохи більшими, ніж у двійкових полях.

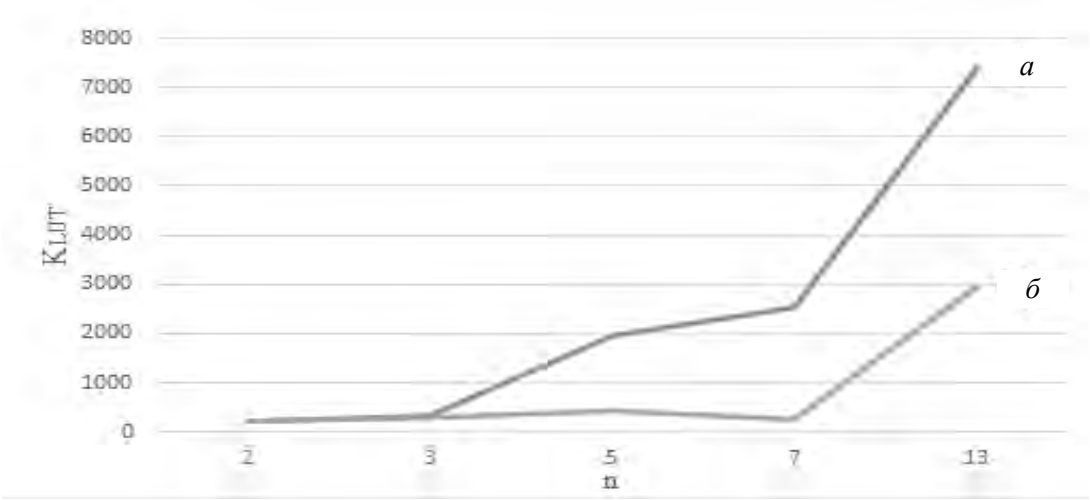


Рис. 3. Графік апаратних затрат помножувачів полів Галуа GF (2^{15}), GF (3^{9}), GF (5^{6}), GF (7^{5}), GF (13^{4}) на ПЛІС Spartan 6: а – з уточненням внутрішньої структури; б – "чорна скринька"

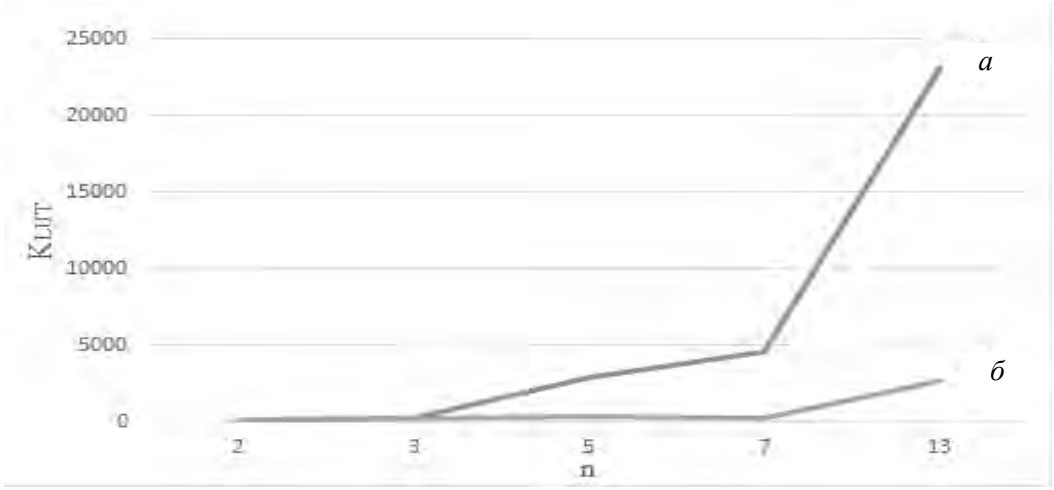


Рис. 4. Графік апаратних затрат помножувачів полів Галуа GF (2^{15}), GF (3^{9}), GF (5^{6}), GF (7^{5}), GF (13^{4}) на ПЛІС Cyclone 5: а – з уточненням внутрішньої структури; б – "чорна скринька"

Таблиця 1

Апаратні затрати LUT та SLICE у разі реалізації помножувачів полів Галуа на ПЛІС Spartan 6

Поле, для якого будується помножувач на ПЛІС Spartan 6	Метод побудови помножувача	К-ть MGC	К-сть елементів у полі порівняно з GF (13^{4})	К-сть витрачених LUT у помно-жувачі	К-сть витрачених SLICE у помно-жувачі	К-сть входів/ виходів	Най-більша затримка ns
1	2	3	4	5	6	7	8
GF (2^{15})	"Чорна скринька"	435	101,3 %	218	82	61	22.161
GF (2^{15})	Помножувач + суматор	435	101,3 %	205	86	61	25.835
GF (3^{9})	"Чорна скринька"	153	96,5 %	312	138	74	31.186
GF (3^{9})	Помножувач + суматор	153	96,5 %	298	106	74	47.267

Продовження табл.1

1	2	3	4	5	6	7	8
GF (5^6)	“Чорна скринька”	66	89,6 %	1946	600	75	49.414
GF (5^6)	Помножувач + суматор	66	89,6 %	439	171	75	42.067
GF (7^5)	“Чорна скринька”	45	95,4 %	2534	963	63	37.389
GF (7^5)	Помножувач + суматор	45	95,4 %	258	103	63	30.513
GF (13^4)	“Чорна скринька”	28	100 %	7395	3031	68	41.970
GF (13^4)	Помножувач + суматор	28	100 %	2949	1018	68	85.703

Таблиця 2

Апаратні затрати LUT та SLICE за реалізації помножувачів полів Галуа на ПЛІС Cyclone 5

Поле, для якого будується помножувач на ПЛІС Cyclone 5	Метод побудови помножувача	К-ть MGC	К-ть елементів у полі порівняно з GF (13^4)	К-ть витрачених ALM у помно-жувачі	К-ть витрачених LAB у помно-жувачі	К-ть входів/ виходів	З’єднан-ня між блоками
GF (2^{15})	“Чорна скринька”	435	101,3 %	122	15	61	406
GF (2^{15})	Помножувач + суматор	435	101,3 %	142	17	61	418
GF (3^9)	“Чорна скринька”	153	96,5 %	292	31	74	543
GF (3^9)	Помножувач + суматор	153	96,5 %	193	24	74	613
GF (5^6)	“Чорна скринька”	66	89,6 %	2879	325	75	6596
GF (5^6)	Помножувач + суматор	66	89,6 %	370	43	75	5345
GF (7^5)	“Чорна скринька”	45	95,4 %	4519	548	63	10450
GF (7^5)	Помножувач + суматор	45	95,4 %	263	32	63	405
GF (13^4)	“Чорна скринька”	28	100 %	23132	3318	68	83624
GF (13^4)	Помножувач + суматор	28	100 %	2660	296	68	50456

З табл. 2 бачимо, що найменші апаратні затрати будуть у поля з основою 2 GF (2^{15}).

Висновки

Здійснено порівняння апаратних затрат помножувачів полів Галуа з основами 2, 3, 5 7, 13 на ПЛІС фірми Xilinx Virtex-7 та Altera – Cyclone-5. В результаті порівняння результатів імплементації

помножувачів видно, що найменші апаратні затрати будуть у помножувачів полів Галуа з основою 2, що не збігається з раніше отриманими теоретичними результатами.

1. Zholubak I. M., Kostik A. T., Glukhov V. S. Features of the processing of elements of the trivial fields of Galois on the modern element base // Bulletin of the Lviv Polytechnic National University "Computer Systems and Networks". – Lviv, 2015. – Issue 830. – P. 27–33. 2. Zholubak I. M., Glukhov V. S. Determination of the extended field of field GF (dm) with the smallest hardware complexity of the multiplier // Bulletin of the Lviv Polytechnic National University "Information systems and networks". – Lviv, 2016. – Vip. 835. – P. 50–58. 3. Zholubak I. M., Glukhov V. S. Hardware costs of Galois field multipliers GF (dm) with a large base // Bulletin of the Lviv Polytechnic National University "Computer Science and Information Technologies". – Lviv, 2017. 4. Glukhov V. S., Elias R. M. Reducing the Structural Complexity of Multisection Multipliers of Galois Field Elements // Electrical and Computer Systems. – 2015. – No. 19 (95). – P. 222–226. 5. Cherkassy M. V., Tkachuk T. I. Characteristics of complexity of devices of multiplication // Radioelectronic and computer systems. – 2012. – No. 5. – P. 142–147. 6. Hlukhov V., Hlukhova A. Galois field elements, multipliers, structural complexity evaluation // Proceedings of the 6th International Conference ACSN-2013. – Lviv, Ukraine. – 2013. – P. 18–19. 7. Glukhov V. S., Trisch G. N. Estimation of structural complexity of multisection multipliers of Galois field elements // Bulletin of the Lviv Polytechnic National University "Computer Systems and Networks". – 2014. – Vip. 806. – P. 27–33. 8. Company Release. New Xilinx Virtex-6 FPGA Family Designed to Satisfy An Insatible Demand for Higher Bandwidth and Lower Power Systems. February 2, 2009. Retrieved February 2, 2009.