УДК 004.382

В. Глухов, А. Костик, М. Шняк
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ОСОБЛИВОСТІ ВИКОНАННЯ ОПЕРАЦІЇ МНОЖЕННЯ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА GF(2^m) ТА GF(3^m)

Описано метод побудови паралельного помножувача елементів трійкових полів Галуа GF(3^m). Запропонований помножувач має каскадну архітектуру. Він може використовуватися в пристроях оброблення цифрових підписів, які ґрунтуються на використанні еліптичних кривих. Описана методика перевірки операцій над елементами полів Галуа GF(p^m) за допомогою математичного пакета Maple.

Ключові слова: поля Галуа GF(3^m), поля Галуа GF(2^m), еліптичні криві, помножувач, цифровий підпис, математичний пакет Maple.

The article describes development of Galois field GF(3^m) elements multiplier. Designed multiplier architecture is scaleable. The multiplier is used in digital signature device which are based on elliptic curves. Also verification method for operations over elements of the Galois fields GF (p^m) with help of mathematical package Maple is described.

Key words: Galois field GF(3^m), Galois field GF(2^m), elliptic curves, multiplier, digital signature, mathematical package Maple.

Вступ

Використання електронних документів відкриває нові можливості в обміні інформацією за допомогою глобальної мережі та периферійних пристроїв. Проте постає проблема щодо захисту електронних документів від можливої модифікації, копіювання, підроблення та маніпуляцій. Для її вирішення необхідні різноманітні засоби та методи захисту інформації. Одним із таких методів захисту інформації є цифровий підпис (ЦП), який за допомогою спеціального програмного забезпечення гарантує автентичність документів, його реквізитів та факту того, що його підписала конкретна особа.

В основу перевірки та отримання цифрового підпису покладено операції над елементами поля Галуа GF(p^q). Реалізація програмних обчислень з використанням універсальних комп'ютерних засобів є не завжди ефективною з погляду швидкодії, зокрема, за необхідності обчислень у реальному часі. Тому актуальною є проблема апаратно-програмної або апаратної реалізації обчислень у скінченних полях Галуа. Забезпечити високу ефективність обчислень у скінченних полях можна лише на основі застосування спеціалізованих обчислювальних засобів. З розвитком інтегральної схемотехніки з'являються нові можливості для реалізації обчислень у полях Галуа з потрібною швидкістю, досяжною лише за рахунок апаратної реалізації операцій [12].

Аналіз публікації

В Україні з 1 січня 2004 року запропоновано використовувати електронний цифровий підпис замість звичайного. Сьогодні використовуються такі стандарти: національний стандарт України ДСТУ 4145-2002 [1], міждержавний стандарт ГОСТ 34.310–95 [2] та міжнародний стандарт IEEE 1363 [3]. У них описано формування цифрового підпису на основі полів Галуа GF(2^m) та еліптичних кривих. Міжнародний стандарт визначає максимальну характеристику поля Галуа $m \leq 998$, тоді як міждержавний стандарт лише m=509. Тому, щоб розвиватись у цій сфері, починають досліджувати трійкові поля Галуа GF(3^m).

Множення є основною операцією для оброблення елементів полів Галуа. У роботах [4], [7], [8] описано методи та алгоритми множення елементів трійкових полів Галуа, але не реалізовано помножувач. Помножувачі можуть бути паралельними, послідовними та паралельно-послідовними. Послідовний помножувач обробляє всі коефіцієнти множеного паралельно на першій стадії, водночас коефіцієнти помножувача обробляються послідовно. А для паралельного помножувача потрібно лише один такт, щоб завершити все множення. Паралельні помножувачі мають велику пропускну здатність і найкраще підходять для розв'язання задач, які потребують високої швидкості обробки і порівняно невеликих скінченних полів [7]. Тому реалізація саме паралельного помножувача для скінченних полів є актуальною і важливою [12].

Існують різноманітні математичні пакети, серед яких Mathcad, Mathlab, Maple, але не всі вони можуть забезпечити роботу з багаторозрядними елементами полів Галуа [10].

Один з найкращих математичних пакетів надає Maple [11]. Цей пакет містить близько трьох тисяч команд, які дають змогу розв'язувати задачі лінійної алгебри, нерівності, диференціальні рівняння, а також дають можливість задавати поля Галуа в цифрових формах, в поліноміальному базисі та виконувати математичні операції над елементами поля.

Постановка задачі

Метою роботи є побудова схеми паралельного помножувача елементів трійкових полів Галуа $GF(3^m)$, а також оцінка можливості перевіряння виконання операцій над елементами розширених полів Галуа за допомогою математичного пакета Maple.

Цифровий підпис

Цифровий підпис повідомлення – це блок даних невеликого розміру, одержаний у результаті криптографічного перетворення повідомлення довільної довжини з використанням особистого (таємного) ключа відправника. В Україні використання цифрового підпису регулюється стандартом ДСТУ 4145-2002 [1]. В основу процедур отримання і перевірки цифрового підпису згідно з цим стандартом покладено операції над елементами поля Галуа $GF(2^m)$, де m – просте число. Популярність цього математичного апарату обумовлена можливістю застосовування порівняно невеликої довжини ключа і блока перетворень щодо інших алгоритмів. Це дає змогу за однакових апаратних витрат на реалізацію пристрою збільшити надійність цифрового підпису. Такий пристрій для опрацювання цифрових підписів, який реалізує криптографічні алгоритми, має ієрархічну структуру (рис. 1) [12].

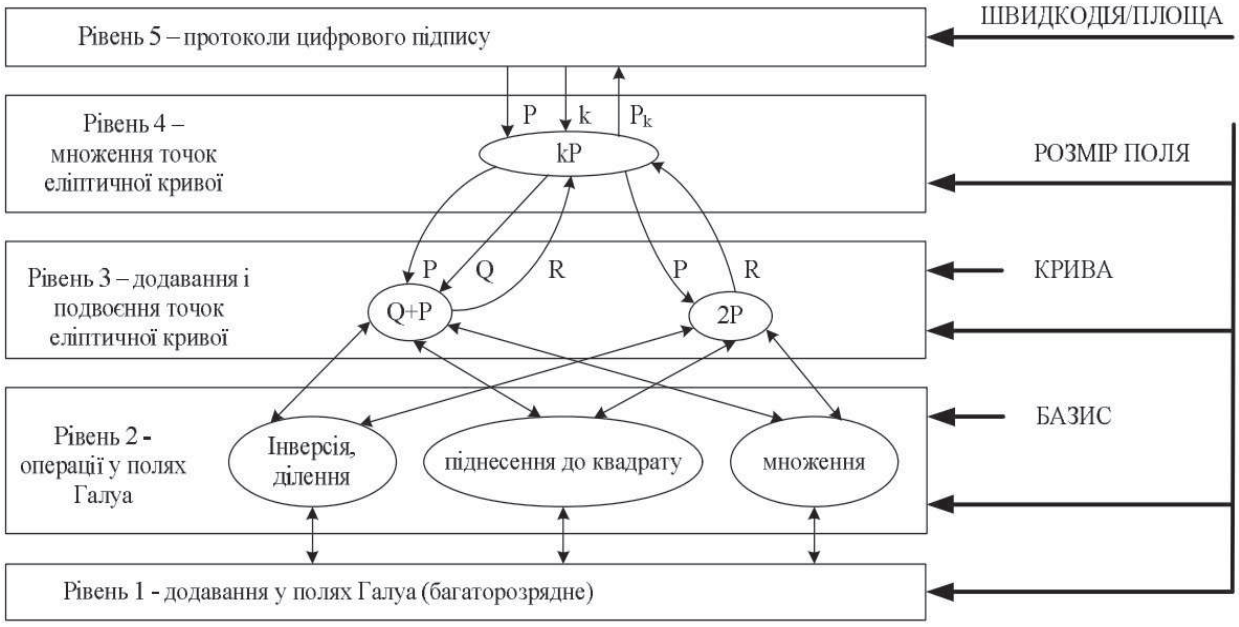


Рис. 1. Ієрархічні рівні алгоритмів

Актуальним залишається питання мінімізації апаратної, обчислювальної, часової, програмної та структурної складностей пристроїв опрацювання цифрових підписів. Хоча сьогодні стандарт дає змогу забезпечити більш ніж достатній рівень захисту, але, зважаючи на швидкий розвиток техніки і математики, актуальною також залишається необхідність його розвитку [6, 12].

Трійкові поля Галуа

Національний стандарт опрацювання цифрових підписів передбачає використання полів Галуа $GF(p^q)$, де p=2. Міжнародні стандарти не виключають використання полів з p=3. Кожний розряд поля $GF(2^m)$ кодується одним бітом, а поля $GF(3^n)$ – двома. Для забезпечення надійності цифрового підпису не меншої, ніж для двійкових полів, порядок n поля $GF(3^n)$ вибирають з умови $n*log3>m$; $n>0{,}6m$ (m – порядок поля $GF(2^m)$) [12].

Для того, щоб було зручно записувати трійкові поля у програмній реалізації, запропоновано [9] таке їх представлення:

Коефіцієнт	0	1	2
Старший біт	0	0	1
Молодший біт	0	1	0

Решту комбінацій вважають недійсними відносно цього представлення.

Спосіб розшарування біта для зберігання коефіцієнтів має певні переваги. Під час програмної реалізації певної задачі коефіцієнти у процесі можуть використовуватись паралельно. За апаратної реалізації можуть бути побудовані ефективні схеми для додавання та множення елементів поля $GF(3^m)$. Програмну та апаратну реалізацію способом розшарування біта запропоновано у [8, 12].

Реалізація паралельного помножувача

Для побудови двійкового поля $GF(2^m)$ використовуються модифіковані комірки Гілда, кожна комірка має 3-бітний вхід та 1-бітний вихід (рис. 2).

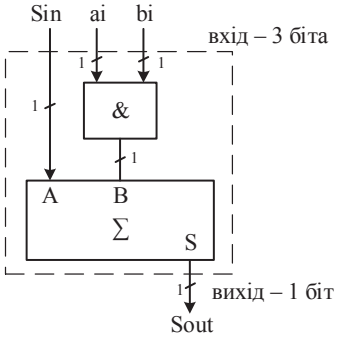


Рис. 2. Модифікована комірка Гілда для $GF(2^m)$

Для побудови трійкового поля $GF(3^m)$ використовуються модифіковані комірки Гілда, які відрізняються від двійкового поля збільшеною кількістю вхідних та вихідних даних. Кожна комірка Гілда має 6-бітний вхід та 2-бітний вихід (рис. 3). Модифікація полягає в тому, що для побудови комірки не використовується перенос.

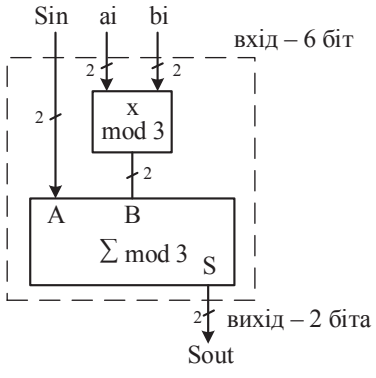


Рис. 3. Модифікована комірка Гілда для $GF(3^m)$

Сама комірка складається із суматора і помножувача за модулем 3.

Синтез суматора за mod 3:

$$S0 = A1\ B1 \vee A0\ \overline{B1}\ \overline{B0} \vee \overline{A1}\ \overline{A0}\ B0$$

$$S1 = A0\ B0 \vee A1\ \overline{B1}\ \overline{B0} \vee \overline{A1}\ \overline{A0}\ B1$$

Синтез помножувача за mod 3:

$$S0 = A0\ B0 \vee A1\ B1$$

$$S1 = A1\ B0 \vee A0\ B1$$

Матриця помножувача для прямого та зворотного ходу поля $GF(2^3)$ зображена на рис. 4. Аналогічну структуру матиме і помножувач для полів Галуа $GF(3^3)$ (рис. 5).

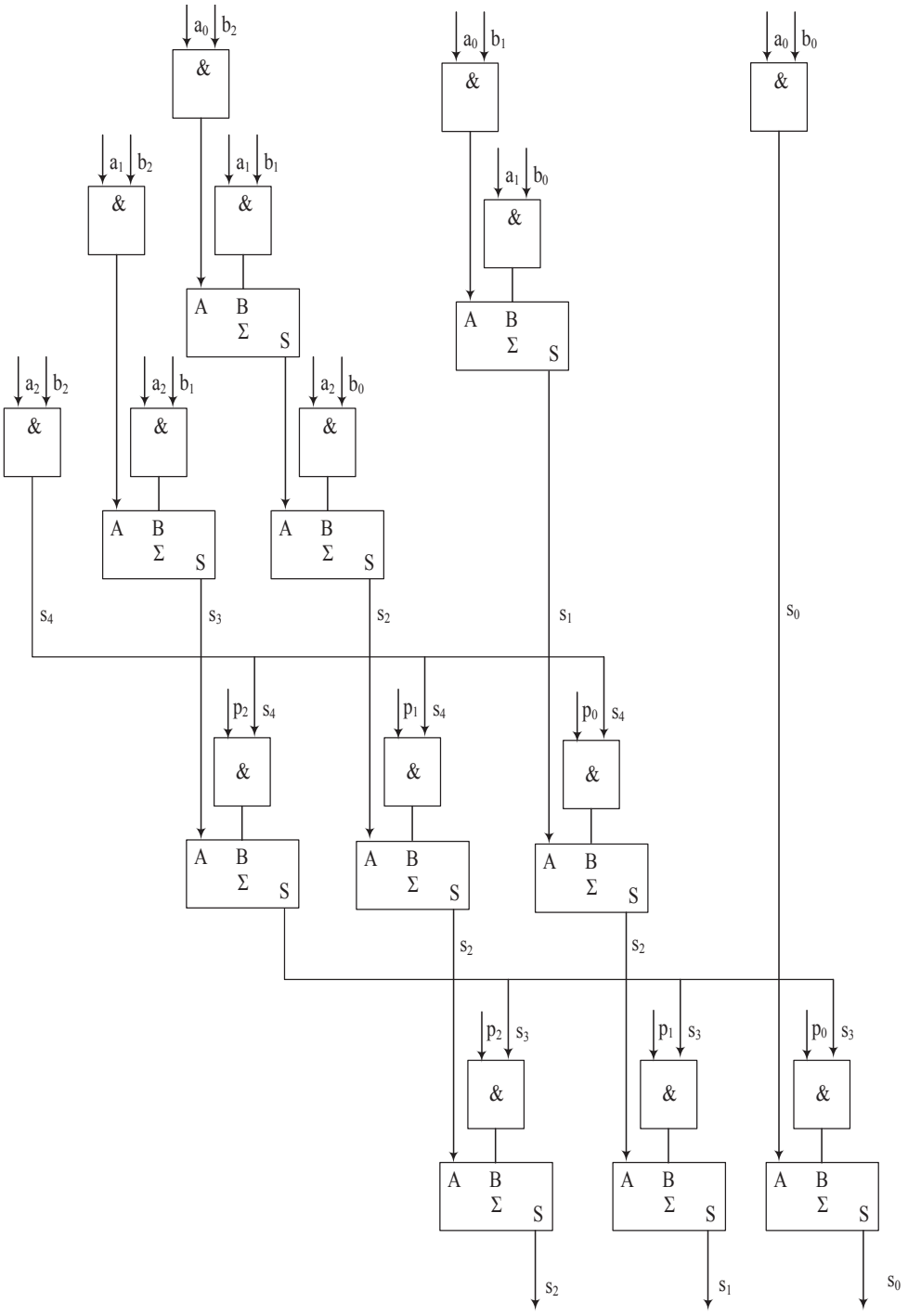


Рис. 4. Матриця помножувача для прямого та зворотного полів $GF(2^3)$

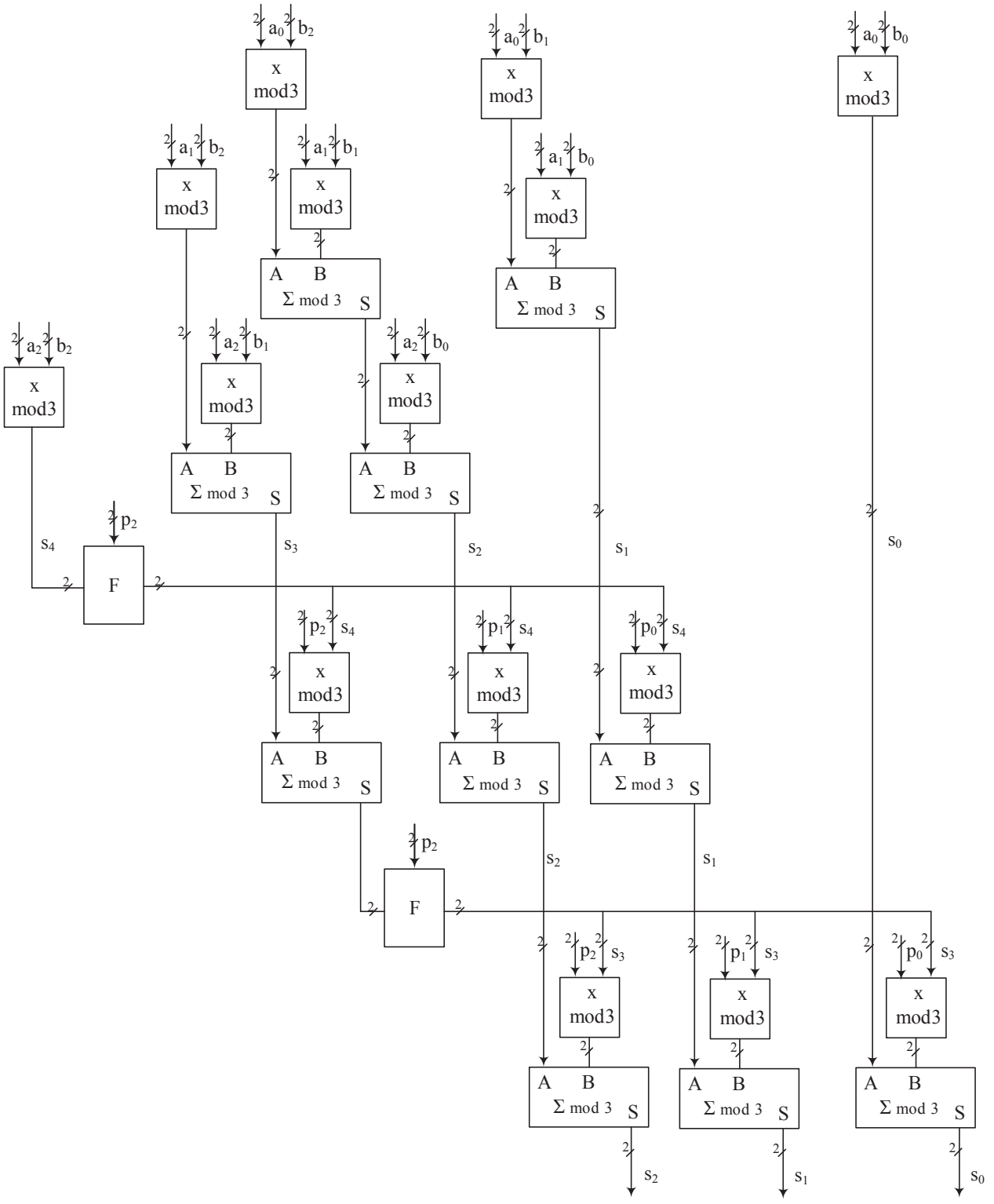


Рис. 5. Матриця помножувача для прямого та зворотного полів GF(3^3)

Перевіряння роботи помножувачів з використанням математичного пакета Maple

Для перевірки правильного виконання операцій у полях Галуа *GF(2^3)* та *GF(3^2)* можна використати математичний пакет Maple.

Для отримання таблиці елементів, представлених у вигляді многочленів, для двійкового та трійкового полів Галуа, заданих поліномами x^3+x+1 та x^2+x+2, відповідно, використовуються такі програми Maple:

```
G:=GF(2,3, x^3+x+1);
 b:= G:-ConvertIn(x);
for i from 0 to 2^3-1 do G:-‘^’(b,i) end do;
```

F_8

$x \bmod 2$
$1 \bmod 2$
$x \bmod 2$
$x^2 \bmod 2$
$(x + 1) \bmod 2$
$(x^2 + x) \bmod 2$
$(x^2 + x + 1) \bmod 2$
$(x^2 + 1) \bmod 2$
$1 \bmod 2$

```
G:=GF(3,2, x^2 + x + 2);
 b:= G:-ConvertIn(x);
for i from 0 to 3^2-1 do G:-‘^’(b,i) end do;
```

F_9

$x \bmod 3$
$1 \bmod 3$
$x \bmod 3$
$(2x + 1) \bmod 3$
$(2x + 2) \bmod 3$
$2 \bmod 3$
$2x \bmod 3$
$(x + 2) \bmod 3$
$(x + 1) \bmod 3$
$1 \bmod 3$

Приклад програм Maple для множення елементів двійкового та трійкового полів Галуа наведено нижче.

```
> G2 := GF(2,3,1+x+x^3):
> Primitive(G2) mod 2;
                    true
> b:=convert("5", decimal, hex);
                    b:=5
> c:=G2[input](b);
              c:= (x^2 + 1) mod 2
> d:=convert("6", decimal, hex);
                    b:=6
> e:=G2[input](d);
              e:= (x^2 + x) mod 2
> f:=G2[`*`](e,c);
              f:= (x + 1) mod 2
> g:=G2[output](f);
                    g:=3
> convert(g, hex);
                     3
```

```
> G3 := GF(3,2,2+x+x^2):
> Primitive(G3) mod 3;
                    true
> b:=convert("5", decimal, hex);
                    b:=5
> c:=G3[input](b);
              c:= (x + 2) mod 3
> d:=convert("6", decimal, hex);
                    b:=6
> e:=G3[input](d);
              e:= 2x mod 3
> f:=G3[`*`](e,c);
              c:= (2x + 2) mod 3
> g:=G3[output](f);
                    g:=8
> convert(g, hex);
                     8
```

У програмі задається двійкове або трійкове поле Галуа, елементи якого подаються в поліноміальному базисі. Для $GF(2^3)$ примітивний многочлен – x^3+x+1, для $GF(3^2)$ – x^2+x+2. За допомогою команди *Primitive(G3) mod p* перевіряють, чи є поліном примітивним за модулем *p*. Операнди *b* та *d* представляються у десятковому коді, виконується їхнє перемноження у вибраному полі. У наведеній програмі у полі $GF(2^3)$ множення виконується над елементами, коди яких подано у десятковій системі: 5_{10} x $6_{10} = 3_{10}$ ($5_{10} = 101_2$, $6_{10} = 110_2$, $3_{10} = 011_3$, тобто результат у двійковому полі $GF(2^3)$: $101_2 x 110_2 = 011_2$), у полі $GF(3^2)$ також множення виконується над елементами, коди яких подано у десятковій системі: 5_{10} x $6_{10} = 8_{10}$ ($5_{10} = 12_3$, $6_{10} = 20_3$, $8_{10} = 22_3$, тобто результат у трійковому полі $GF(3^2)$: 12_3 x $20_3 = 22_3$). Реалізація операцій множення елементів полів Галуа в математичному пакеті Maple дає змогу використовувати його для перевірки правильності виконання основних операцій у двійкових та трійкових полях за їх апаратної реалізації на ПЛІС.

Для виконання множення елементів полів Галуа важливо знайти незвідні многочлени, що утворюють поле. Ця операція потребує значних часових витрат, особливо для полів з великим порядком. За допомогою математичного пакета Maple можна знайти такі поліноми для вибраного поля, а також оцінити час їх знаходження, що дає змогу непрямим способом оцінити складність опрацювання елементів вибраного поля. Для цього використовуються команди *Nextprime* та *time*.

Таке тестування проводилося на ноутбуку Sony VAIO з характеристиками: процесор Intel Core i3-3120M, тактова частота ЦП – 2.50GHz, пам'ять – 2500 МГц, кількість ядер – 2, кількість логічних процесорів – 4.

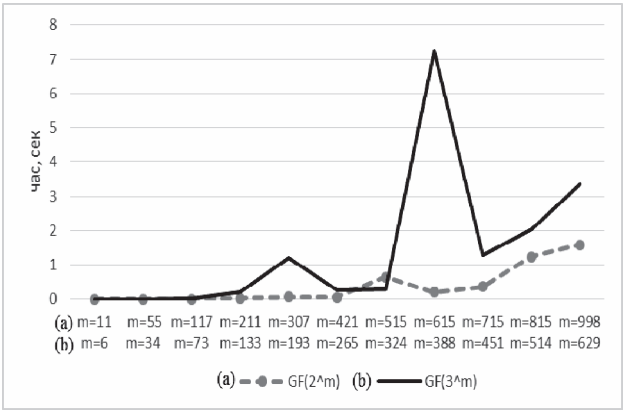
У табл. 1 показано порівняння часу знаходження многочленів, що утворюють поле, для полів Галуа з основами 2, 3, 5, 7, 11, 13 та різними порядками. Величину порядку m у кожному стовпці вибрано з умови приблизної рівності кількості елеметів у полі $GF(p^m)$. Графічні залежності часу обчислення незвідних многочленів відображено на рис. 6.

Таблиця 1

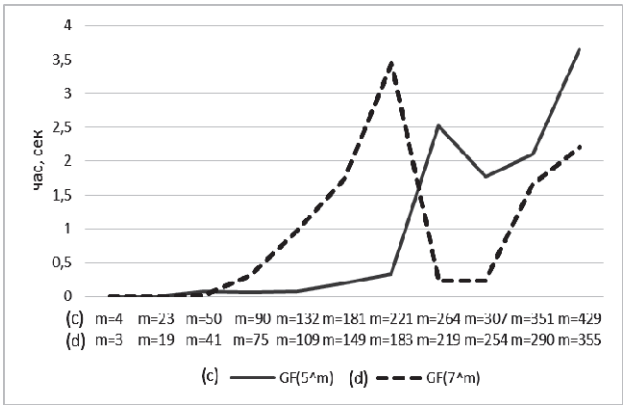
Час обчислення незвідних многочленів для полів Галуа $GF(p^m)$

№ з/п	p	m / Час виконання										
1	**2**	998	815	715	615	515	421	307	211	117	55	11
		1,578	*1,234*	*0,359*	*0,203*	*0,64*	*0,046*	*0,062*	*0,031*	*0*	*0*	*0*
2	**3**	629	514	451	388	324	265	193	133	73	34	6
		3,343	*2,046*	*1,281*	*7,234*	*0,296*	*0,25*	*1,203*	*0,203*	*0,015*	*0*	*0*
3	**5**	429	351	307	264	221	181	132	90	50	23	4
		3,656	*2,109*	*1,765*	*2,515*	*0,328*	*0,203*	*0,078*	*0,062*	*0,078*	*0*	*0*
4	**7**	355	290	254	219	183	149	109	75	41	19	3
		2,203	*1,656*	*0,234*	*0,234*	*3,437*	*1,734*	*0,984*	*0,312*	*0,015*	*0*	*0*
5	**11**	289	235	206	177	148	121	88	60	33	15	2
		7,062	*4,234*	*4,14*	*0,296*	*1,703*	*0,656*	*0,171*	*0,031*	*0,015*	*0*	*0*
6	**13**	269	220	193	166	139	113	82	57	31	14	2
		3,39	*0,39*	*8,171*	*0,093*	*0,156*	*1,671*	*0,031*	*0,046*	*0,046*	*0*	*0*

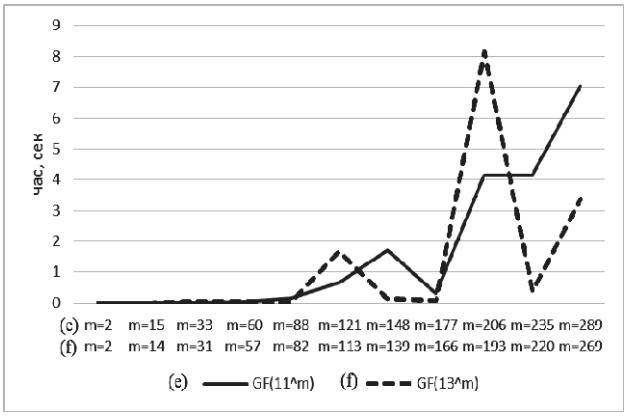
З рис. 6 видно, що існують поля з високою і низькою часовою складністю обчислення незвідних поліномів, що непрямим способом вказує на можливі ускладнення під час опрацювання елементів окремих полів. Поля з вищим порядком можуть мати меншу часову складність.



а) $GF(2^m)$ та $GF(3^m)$

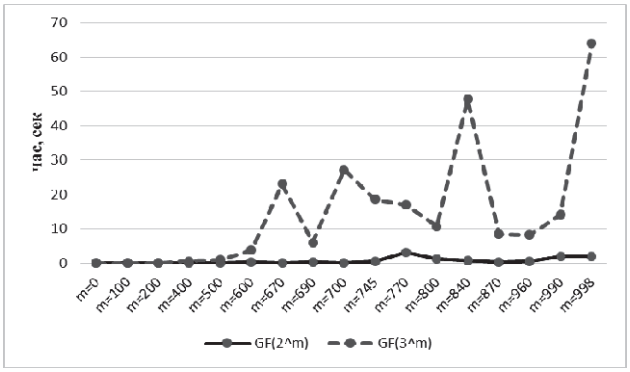


б) $GF(5^m)$ та $GF(7^m)$

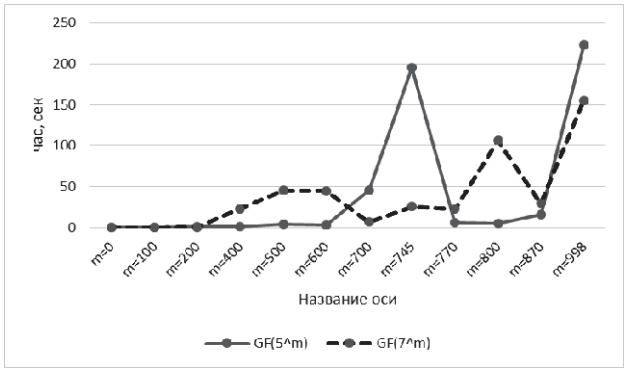


в) $GF(11^m)$ та $GF(13^m)$

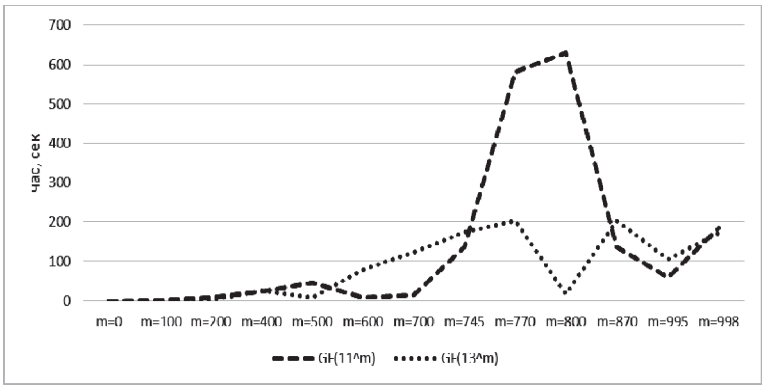
Рис. 6. Час обчислення незвідних многочленів для полів Галуа $GF(p^m)$



а) поле GF(2^m) та GF(3^m)



б) поле GF(5^m) та GF(7^m)



в) поле GF(5^m) та GF(7^m)

Рис. 7. Порівняння полів Галуа за часом повернення незвідних многочленів з однаковими степенями

На рис. 7 зображено час знаходження незвідного многочлена для полів Галуа GF(2^m) та GF(3^m) (рис. 7, *а*), GF(5^m) та GF(7^m) (рис. 7, *б*), GF(11^m) та GF(13^m) (рис. 7, *в*) з однаковими степенями m (табл. 2).

Таблиця 2

Час знаходження незвідного многочлена, с

Поле GF	m=100	m=200	m=400	m=500	m=600	m=700	m=800	m=998	m=2000
GF(2^m)	0	0,015	0,078	0,187	0,281	0,031	1,281	1,89	36,312
GF(3^m)	0,062	0,078	0,562	0,921	3,843	27,218	10,765	64	452,328
GF(5^m)	0,015	1,218	1,093	4,484	2,703	45,515	5,14	223,156	302,796
GF(7^m)	0,156	0,296	23,328	45,359	45,015	6,75	106,484	155	1133,906
GF(11^m)	1,031	7,546	24	46,078	7,234	15,14	630,968	185,937	504,359
GF(13^m)	0,109	2,343	26,203	7,468	79,078	122,67	16,5	171,562	1505,906

Реалізація модифікованих комірок Гілда на ПЛІС

Модифіковані комірки Гілда планується реалізувати на комбінаційних елементах ПЛІС (LUT). LUT сучасних ПЛІС *Spartan6* мають шість входів та один вихід. Кількість модифікованих комірок Гілда для побудови паралельного помножувача дорівнює kq^2 (де k – коефіцієнт пропорційності), для поля $GF(2^m)$ кожна комірка Гілда має 3-бітний вхід і 1-бітний вихід. Відповідно, кількість LUT $N_2 = km^2$. Для поля $GF(3^n)$ кожна модифікована комірка Гілда має 6-бітний вхід і 2-бітний вихід. Відповідно, кількість LUT $N_3 = 2kn^2$.

Тоді коефіцієнт співвідношення апаратних витрат дорівнює

$$s = N_2/N_3 = km^2/2kn^2 = m^2/2*(0{,}6m)^2 = 1{,}4 > 1.$$

Тобто на сучасній елементній базі апаратні витрати на реалізацію паралельного помножувача для елементів трійкового поля Галуа менші, ніж для його реалізації у двійковому полі [5], [12].

Висновки

Розглянута побудова паралельного помножувача на основі модифікованих комірок Гілда. Доведено його переваги над аналогічним помножувачем елементів двійкових полів Галуа GF(2^m). Показано схемотехнічну реалізацію комірки Гілда. Показано можливість перевірки виконання операцій над елементами розширених полів Галуа за допомогою математичного пакета Maple. Показано, що існують поля з високою і низькою складністю виконання операцій знаходження незвідних поліномів, причому поля з вищим порядком можуть мати меншу часову складність.

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003. 2. Межгосударственный стандарт ГОСТ 34.310.95. Информационная технология. Криптографическая защита информации. Процедура выработки проверки ЕЦП на базе асимметрического алгоритма. – Минск: Госстандарт Украины, с дополнениями, 1997. 3. IEEE 1363-2000: Standard Specifications For Public Key Cryptography. 2000. The Institute of Electrical and Electronics Engineers, Inc. Електронная подпись. 4. Глухов В. С. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа GF(2^m) з надвеликим степенем / В. С. Глухов, Р. М. Еліас, А. О. Мельник // Комп'ютерно-інтегровані технології: освіта, наука, виробництво // Луцький національний технічний університет. – 2013. – Луцьк. – № 12. – С. 103–106. 5. Глухов В. С., Костик А. Т. Використання сучасних ПЛІС для опрацювання елементів полів Галуа (p^q): тези для 9-ї наук. конф. ХУПС. – 2013. – 178 с. 6. Еліас Р. М. Методи та засоби проектування конфігуровних секційних операційних пристроїв для опрацювання цифрових підписів: автореф. дис. ... канд. техн. наук: 05.13.05 – комп'ютерні системи та компоненти / Родріг Метрі Еліас ; Національний університет «Львівська політехніка». – Львів, 2013. – 26 с. 7. Steininger A., Serra M. Reconfigurable Hardware Implementation of Polynomial Arithmetic over the Finite Field GF(3), Institute 182-1, Vienna University of Technology, 2006. 8. Merchan J. G. Arithmetic Architectures for Finite Fields GF(p^m) with Cryptographic Applications. Bochum, 2004. 9. Deschamps J. P., Imana J. L, Gustavo D. Hardware Implementation of Finite-Field Arithmetic. 2009 The McGraw-Hill Companies, Inc., pp. 347. 10. Берко Т., Глухов В. Перевірка пристроїв для обробки цифрових підписів, що ґрунтуються на еліптичних кривих // Технічні новини: наук.-соц. журнал, орган Українського інженерного товариства у Львові. – Львів. – 1, 2:25, 26(2007), 53–57. 11. Математичний пакет Maple [Електронний ресурс]. – Режим доступу: http://www.maplesoft.com. 12. Шняк М. М. Помножувач елементів трійкових полів Галуа // [Електронний ресурс] 73-тя студентська наук.-техн. конф. (СНТК), жовтень, Львів, 2015. – Режим доступу: http://eom.lp.edu.ua/sntk/ .