МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

**Рахма Мохаммед Кадім Рахма**

УДК 004.31

# ДИСЕРТАЦІЯ

# МОДЕЛІ ТА МЕТОДИ ПОБУДОВИ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

05.13.05 – Комп'ютерні системи та компоненти
05 – Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Рахма Мохаммед Кадім Рахма

Науковий керівник:
Глухов Валерій Сергійович
доктор технічних наук, професор

***Ідентичність усіх примірників дисертації***
**ЗАСВІДЧУЮ**

*Вчений секретар спеціалізованої*
*вченої ради Д 35.052.08* */Луцик Я. Т./*

Львів-2019

# АНОТАЦІЯ

*Рахма Мохаммед Кадім Рахма* Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Національний університет «Львівська політехніка», Львів, 2019.

У дисертації розв'язується важливе науково-технічне завдання - здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

У **Вступі** викладено сучасний стан завдання, обґрунтовано актуальність побудови операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, сформульовано мету та задачі досліджень, описано основні наукові результати та показано їх практичне значення, представлено зв'язок роботи з науковими програмами, планами, темами. Наведено відомості про апробацію, публікації та використання результатів досліджень.

У **першому** розділі проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП). У розділі розглянуто сучасний стан розвитку комп'ютерних систем, який характеризується виникненням кіберфізичних систем (КФС). Розглянуто алгоритмічні основи проєктування комп'ютерних засобів КФС. Виділено програмно-апаратну SH-модель алгоритму. Відмічено переваги апаратних реалізацій алгоритмів.

Серед методів забезпечення захисту інформації КФС розглянуто криптографію еліптичних кривих з її націленістю на опрацювання електронних цифрових підписів. Відмічено вплив технологій квантових обчислень на

використання еліптичних кривих у КЗІ. З цієї точки зору також розглянуто криптографію ізогеній суперсингулярних еліптичних кривих, яка може протистояти використанню квантових комп'ютерів.

Розглянуто використання розширених полів Галуа GF(pm) як математичної основи електронних цифрових підписів та методи оцінювання складності пристроїв опрацювання елементів полів Галуа.

Як елементну базу для побудови згаданих вузлів розглянуто ПЛІС, ядра (VHDL-описи моделей функціональних вузлів) для них та генератори ядер. З цією метою проаналізовано методи генерації описів функціональних вузлів.

З метою забезпечення якості засобів КЗІ розглянуто можливості використання математичних пакетів для проведення обчислень у розширених полях Галуа. Найкращим визначено пакет Maple (Waterloo Maple Inc.). Розглянуто необхідність маскування роботи засобів КЗІ як один з методів захисту від атак на них.

**Другий** розділ присвячено вибору та обґрунтуванню напряму досліджень та проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, у розділі наведено методи вирішення поставлених задач, визначено загальну методику проведення досліджень. Також виконується наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

Метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ пропонується як метод знаходження розширеного поля Галуа, у якому обрані характеристики СП будуть найкращими, що забезпечить створення СП для «найкращого» поля (далі цей термін буде вживатися без лапок). Підхід базується на оцінювання складностей одного з найважливіших вузлів СП - помножувача.

Порядок застосування методу: обирається розширене поле Галуа; обирається базис представлення елементів полів Галуа; обираються базові елементи помножувача; обирається структура базових елементів; обирається структура

помножувача; проводиться аналіз обраного типу складності, відносні значення параметрів складності формуються по відношенню до аналогічних параметрів розширеного двійкового поля; дослідження повторюються для всіх обраних для аналізу розширених полів Галуа; фіксуються результати дослідження; визначається найкраще поле.

Як складові частини метод містить наступні методи, на яких проводиться аналіз обраного типу складності..

1. Оцінювання часової складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$.

2. Оцінювання структурної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ у нормальному та поліноміальному базисах.

3. Оцінювання ємнісної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$.

Метод оцінювання складності злому апаратних засобів КЗІ також розглянуто в цьому розділі.

У розділі представлено метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі.

У **третьому** розділі досліджено можливість апаратної реалізації операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК як багаторівневих систем. У розділі проведено апаратну реалізацію алгоритмів роботи засобів КЗІ. Запропоновано структуру спецпроцесора для опрацювання елементів розширених полів Галуа. Протокольні процесори у цій дисертаційній роботі не розглядаються так само як і інтерфейс між ними та СпП. Запропоновано модель одного із СП для опрацювання елементів полів Галуа (GF-процесор). Запропонований GF-процесор має додатковий функціональний блок для розміщення досліджуваних ядер, варіанти ядер порівнювалися за величиною апаратних витрат на реалізацію функціонального блока FU. Для проведення досліджень у ході виконання роботи було розроблено технологічний засіб (генератор ядер) для

проєктування помножувачів елементів полів Галуа *GF(pm)* для поліноміального базису, вузлів обчислення квадратних коренів, інверторів з незалежним від операндів часом обчислення. Основні параметри генератора, які може встановити користувач: тип ядра; метод створення ядра (інвертора - від 1 до 5); характеристика p ($2 \leq p \leq 21000$) розширеного поля Галуа *GF(pm);* степінь m ($3 \leq m \leq 1000$) розширеного поля Галуа *GF(pm);* незвідний многочлен F, що утворює поле. При цьому порядок поля *pm* не може перевищувати значення 21000 ($pm \leq 21000$). Відсутні в моделі GF-процесора ядра схемотехнічно зібрано у додатковому функціональному вузлі (FU). Реалізовані відповідно до запропонованих методів інвертування ядра інверторів з незалежним від операндів часом обчислення досліджуються в поліноміальному базисі двійкових полів Галуа GF(2m) з метою вибору найкращого за апаратною та часовою складностями. Необхідні для інвертування додаткові елементи GF-процесора займають від 119 до 919 слайсів і забезпечують час інвертування від 131 до 8629 нс (GF(264)), що дозволяє обирати ядра в залежності від потреб замовника.

Четвертий **розділ** присвячено впровадженню операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом). Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та

«Системне програмування»).

**Ключові слова:** кіберфізичні системи, розширені поля Галуа, еліптичні криві, модифікована комірка Гілда, вбудований контроль, маскування.

## ABSTRACT

Rahma Mohammed Kadhim Rahma. Models and methods for constructing operating units for Galois fields used in cryptographic data protection based on elliptic curves. – Qualification scientific work on the rights of a manuscript.

The thesis for a candidate of technical science (Ph.D.) degree in specialty 05.13.05 «Computer systems and components». – Lviv Polytechnic National University, Lviv, Ukraine, 2019.

The dissertation is devoted to the solution of the scientifically applied problem of creation of operating units for Galois fields used in cryptographic data protection on the basis of elliptic curves.

The introduction outlines the current state of the task, substantiates the relevance of the construction of operating nodes for the Galois fields, which are used in data protection based on elliptic curves, the purpose and objectives of the research are formulated, basic scientific results are described and their practical significance is shown, the connection of this work with scientific programs, plans, topics is presented. Information on testing, publication and use of research results is provided.

The first section provides a systematic analysis of the current state of the theory, methods and means of designing specialized computers, data protection devices, analysis of the most important open standards and algorithms for them, generalized structures of special processors (SP). This section discusses the current state of computer systems development, which is characterized by the emergence of cyber physical systems (CPS). The algorithmic basics of designing CPS computer tools are considered. The software and hardware SH-model of the algorithm is highlighted. Advantages of hardware implementations of algorithms are noted. Elliptic curve cryptography with its focus on digital signature processing has been considered among the methods of data security in

CPS. The influence of quantum computing technologies on the use of elliptic curves in data protection is noted. From this point of view, cryptography of isogenes of supersingular elliptic curves, which can resist the use of quantum computers, is also considered.. The use of extended Galois fields GF($p^m$) as a mathematical basis for digital signatures is considered. Also methods for evaluating the complexity of devices for processing Galois elements are considered.

FPGAs, cores (VHDL descriptions of models) for them, and core generators are considered as the element base for the construction of the mentioned units. For this purpose, methods for generating descriptions of functional units are analyzed.

In order to ensure the quality of data protection, the possibility of using mathematical packages to perform calculations in the extended Galois fields is considered. Maple is best identified (Waterloo Maple Inc.). The necessity of masking the work of data protection means as one of the methods of protection against attacks against them is considered.

The second section is dedicated to the selection and justification of the direction of research and design of operating units for Galois fields used in data protection based on elliptic curves, the section presents methods for solving problems, defines a general methodology for research. There is also a scientific justification for the feasibility of using operating units for Galois fields used in data protection based on elliptic curves, it also identifies the fields that are best used to accomplish this task, as well as the creation of methods and means of designing and comparing the mentioned nodes is carried out.

The method for estimating the complexity of Galois extended element multiplier models is proposed as a method of finding the field in which the selected multiplier characteristics will be the best, that will create a multiplier for the "best" field (hereinafter referred to as the term without quotes). The approach is based on evaluating the complexity of one of the most important units of the processor - the multiplier.

The procedure for applying the method: an extended Galois field is selected; the basis for representing the elements of the Galois fields is selected; the basic elements of the multiplier are selected; the structure of the basic elements is selected; the structure of the multiplier is selected; the selected type of complexity is analyzed; relative values of

complexity parameters are formed with respect to similar parameters of the extended binary field; studies are repeated for all selected to analyze extended Galois fields; the results of the study are recorded; the best field is determined.

As components, the method contains the following methods, which analyze the selected type of complexity.

1. Estimation of time complexity of Galois extended element multiplier models.

2. Estimation of structural complexity of extended Galois fields elements multipliers models in normal and polynomial bases.

3. Estimation of the capacitance complexity of the Galois extended element multiplier models.

A method for assessing the complexity of hacking data protection hardware is also discussed in this section.

This section presents a method of masking the operation of hardware for finding inverted elements in extended binary Galois fields in a polynomial basis.

The third section explores the feasibility of hardware implementation as multilevel systems of operating units for Galois fields used in data protection based on elliptic curves. This section describes the hardware implementation of data protection algorithms. The structure of the special processor for processing elements of extended Galois fields is proposed. The protocol processors in this dissertation are not considered in the same way as the interface between them and the special processor. A model of one of the special processors for processing Galois elements (GF-processor) is proposed. The proposed GF-processor has an additional functional unit to accommodate the cores under study, cores variants were compared in terms of hardware cost to implement the FU functional unit. For research in the course of work, a technological tool (core generator) was developed to create Galois field element multipliers for polynomial basis, square root computing units, inverters with operand-independent computation time. The basic parameters of the generator that can be set by the user are: core type; core creation method; characteristic p ($2 \le p \le 2^{1000}$) of the extended Galois field $GF(p^m)$; the degree m ($3 \le m \le 1000$) of the extended Galois field $GF(p^m)$; irreducible polynomial F that forms a field. However, the order $p^m$ of the field cannot exceed the value $2^{1000}$ ($p^m \le 2^{1000}$). cores, that are not present in

the GF-processor model, are schematically assembled in an additional functional unit (FU). The cores, which have an operand-independent computation time, are implemented according to the proposed inversion methods, and are investigated in the polynomial basis of the extended Galois binary fields to select the best one with hardware and time complexity. The additional GF processor elements required for inversion take from 119 to 919 slices and provide an inversion time from 131 to 8629 ns (for GF($2^{64}$)), allowing you to select cores according to customer needs.

The fourth section is devoted to the implementation of operational cores for the Galois fields, which are used for data protection based on elliptic curves.

The scientific provisions and conclusions of the dissertation have been successfully used during the project work at the firm AL-NABAA Network Solution L.L.C. (Baghdad, Iraq), which is confirmed by the relevant Act, and when conducting state budget research work of DB / CYBER «Integration of methods and means of measurement, automation, processing and protection of information in the base of cyber-physical systems» (state registration number 0115U000446), which is also confirmed by the relevant Act). Also, the results of the dissertation were used at the Department Computers of the Institute of Computer Technologies, Automation and Metrology of the Lviv Polytechnic National University in preparation and teaching of lectures and laboratory works of the discipline «Research and design of computer systems and networks» (для educational qualification level "Master", specialty 123 «Computer Engineering», for Computer Systems and Networks, Cyberphysical Systems, and System Programming majors).

**Keywords**: cyberphysical systems, extended Galois fields, elliptic curves, modified Guild cell, built-in control, masking.

## СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації:

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

2. Рахма, М. Структурна складність помножувачів елементів полів Галуа у

нормальному та поліноміальному базисах / Р. Еліас, М. Рахма, В. Глухов / Електротехнічні та комп'ютерні системи. – Одеса: – 2017. Вид-во Наука і техніка. - № 25 (101). – С. 332-340.

3. Rahma, M. Galois Fields Elements Processing Units for Cryptographic Data Protection in Cyber-Physical Systems / V. Hlukhov, I. Zholubak, A. Kostyk, M. Rahma / Advances in Cyber-Physical Systems, Вид-во Національного університету Львівська політехніка. - Volume 2, Number 2, 2017. – pp. 47- 53.

4. Rahma, M. FPGA cores for fast multiplicative inverse calculation in Galois Fields / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 27(103), с. 227-233.

5. Рахма, М. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Р. М. Еліас, В. С. Глухов, М. Рахма, І. М. Жолубак / Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 905. Львів, 2018. С. 64-72.

6. Рахма, М. Ємнісна складність та вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Родріг Еліас, Валерій Глухов, Мохаммед Рахма, Іван Жолубак / Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 29(105), с. 95-102.

7. Rahma, Mohammed Kadhim. Galois Field Operational unit For Elliptic Curve Cryptography Digital Signature. V Міжнародний молодіжний науковий форум "Litteris et Artibus". 26–28 листопада, 2015. Україна, Львів. Pp. 66-71.

8. Rahma, Mohammed Kadhim. Time complexity of multipliers for Galois fields / Mohammed Kadhim Rahma, Valeriy S.Hlukhov / INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24-26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52-53.

9. Рахма, М.К.Р. Часова складність орієнтованих на виконання криптографічних перетворень в складі кіберфізичних систем помножувачів на основі модифікованих комірок Гілда / Глухов В.С., Еліас Р.М., Рахма М.К.Р / Матеріали другого наукового семінару Кібер-фізичні системи: досягнення та

виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р. С. 36-42.

10. Рахма, М. Аналіз можливості побудови багатосекційних помножувачів елементів полів Галуа для нормального та поліноміального базисів / В. С. Глухов, Р. Еліас, М. Рахма / Матеріали третього наукового семінару Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 13-14 червня 2017 р. С. 38-47.

11. Rahma, M. Computing Square Roots and Solve Equations of ECC over Galois Fields /M. Rahma, V. Hlukhov / International Youth Science Forum ”Litteris Et Artibus”, November 23-25, 2017, Lviv, Ukraine, pp. 437-440.

12. Rahma, Mohammed Kadhim. Automation System for Configuration of Cryptographic Data Protection Unit Model / Ivan Zholubak, Mohammed Kadhim Rahma and Valeriy Hlukhov / Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv, pp. 669-679.

13. Rahma, Mohammed Kadhim. Automation System for Configuration of Cryptographic Data Protection Unit Model / Ivan Zholubak, Mohammed Kadhim Rahma and Valeriy Hlukhov / Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv, pp. 669-679.

14. Rahma, Mohammed. Devices for Multiplicative Inverse Calculation in Binary Galois Fields / Valeriy Hlukhov, Mohammed Rahma and Ivan Zholubak. / Proceedings of 9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT’2018. Kyiv, May 24-27, pp. 275-278.

15. Rahma, Mohammed. Hardware components for post-quantum elliptic curves cryptography / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. / Proceedings of International Conference "Advanced Computer Information Technologies", June 1-3, 2018 in Ceske Budejovice, Czech Republic, pp. 236-239.

16. Рахма, Мохаммед Кадім Рахма. Принципи побудови та проектування операційних вузлів для полів Галуа, що використовуються в задачах

криптографічному захисті інформації на основі еліптичних кривих / В.С. Глухов, І.М. Жолубак, Мохаммед Кадім Рахма Рахма / Кіберфізичні системи: багаторівнева організація та проектування [Текст]: монографія – А.О. Мельник та інші. За редакцією професора А. О. Мельника. Львів: «Магнолія 2006», 2019. 238 с. С. 58-131. 41 17

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | |
|---|---|
| АЛП | арифметико-логічний пристрій |
| ЕК | еліптична крива |
| ЕЦП | електронно-цифровий підпис |
| КЗ | комп'ютерний засіб |
| КЗІ | криптографічний захист інформації |
| КП | криптопроцесор |
| КС | комп'ютерна система |
| КФС | кіберфізична система |
| НВІС | надвелика інтегральна схема |
| ПЛІС | програмована логічна інтегральна схема |
| ПрП | протокольний процесор |
| СК | система команд |
| СО | спецобчислювач |
| СКС | спеціалізована комп'ютерна система |
| СП | спеціалізований процесор, спецпроцесор |
| СпП | співпроцесор |
| ЦП | центральний процесор |
| ШП | шифропроцесор |
| AUC | *Arithmetic Unit Controller* – контролер арифметичного вузла |
| DSA | *Digital Signature Algorithm* - криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису |
| ECC | Elliptic-Curve Cryptography - еліптична криптографія |
| ECDSA | *Protocol Elliptic Curve Digital Signature Algorithm* – алгоритм цифрового підпису, що використовує еліптичні криві |
| $GF(p^m)$ | *Galois Field* – поле Галуа, $p$ – характеристика поля, просте число, $m$ – степінь поля, натуральне число (якщо m=1 – поле просте, якщо m > 1 – поле розширене), $p^m$ – порядок поля |
| IP | *Intellectual property* - інтелектуальна власність |
| LUT | *Look-Up-Table,* програмовна комбінаційна схема в складі ПЛІС |
| MC | *Main Controller* – головний контролер |
| OSI | *Open Systems Interconnection* – взаємозв'язок відкритих систем |
| RSA | абревіатура від прізвищ *Rivest*, *Shamir* та *Adleman,* криптографічний алгоритм з відкритим ключем |
| SoM (SOM) | *System on Module* – система на модулі |
| SoC (SOC) | *System on Chip* – система на кристалі |
| VC | *Virtual Components* - віртуальні компоненти |
| $\lceil x \rceil$ | Результат заокруглення числа $x$ до найближчого більшого цілого |

# ВСТУП

**Актуальність роботи.** Сучасний етап розвитку комп'ютерних технологій характеризується виникненням, розвитком і впровадженням кіберфізичних систем (КФС), а також підготовкою до появи серійних квантових комп'ютерів. Поява і розвиток КФС, однією з головних рис яких є використання бездротових технологій, гостро ставить питання захисту інформації, яку опрацьовують ці системи. Постійне зростання продуктивності комп'ютерів, поява нових технологій та алгоритмів, впровадження нової елементної бази може бути використано зловмисниками для порушення інформаційної безпеки. Це зумовлює необхідність пошуку нових, більш надійних методів криптографічного захисту інформації (КЗІ) та маскування їхньої роботи. Бажано, щоб ці методи ґрунтувалися на вже відомих технологіях і засобах і покращували їхню дієвість. Сьогодні одним з методів КЗІ є використання цифрових підписів, які базуються на алгоритмах опрацювання точок еліптичних кривих (ЕК) і елементів розширених двійкових $GF(2^m)$ та простих $GF(p)$ полів Галуа. Можливості квантових комп'ютерів роблять небезпечним використання існуючих алгоритмів, що базуються на використанні ЕК. Хоча потужні квантові комп'ютери ще не з'явилися, вже ведеться пошук алгоритмів КЗІ, які залишаться надійними і в еру квантових комп'ютерів. Одним із можливих методів є метод, що базується на використанні ізогеній суперсингулярних ЕК у полі Галуа $GF(2^m)$, для обчислення яких використовуються ті ж самі операції, що і в сучасних алгоритмах цифрового підпису, які базуються на використанні полів Галуа $GF(2^m)$. Крім двійкових полів $GF(2^m)$ можна використовувати й інші розширені поля Галуа $GF(p^n)$, такі, що $2^m \approx p^n$. При опрацювання кодів елементів згаданих полів Галуа необхідно виконувати опрацювання двійкових кодів, довжина яких приблизно дорівнює $m$ (за сучасними стандартами $m$ може досягати значення 1000). Саме в опрацюванні таких кодів полягає призначення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, та які утворюють назву цієї дисертаційної роботи. У дисертації розв'язується важливе науково-технічне завдання - здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще

використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів. Особливістю алгоритмів КЗІ є їхня багаторівнева структура, де на різних рівнях виконуються специфічні математичні операції над багаторозрядними кодами: операції над елементами простих *GF(p)* та розширених *GF(pm)* полів Галуа, операції над точками еліптичних кривих. В залежності від умов використання необхідно забезпечувати конфігурацію операційних пристроїв, які реалізують вказані алгоритми: забезпечувати зміну поля Галуа, базису для представлення елементів поля, зміну еліптичної кривої.

В Україні використання операцій над елементами полів Галуа регулюється стандартами опрацювання цифрових підписів ДСТУ 4145-2002 та ДСТУ ISO/IEC 15946-1: 2015, в основу яких покладено операції над точками несингулярних еліптичних кривих у полі Галуа GF(2m). Популярність цього математичного апарату обумовлена можливістю застосовування відносно невеликої довжини ключа і блоку перетворень по відношенню до інших алгоритмів. Це дає змогу при однакових апаратних витратах на реалізацію пристрою збільшити надійність цифрового підпису. Тому актуальним залишається питання мінімізації обчислювальної, апаратної, часової, структурної та програмної складностей. Хоча на сьогоднішній день стандарт дозволяє забезпечити більш ніж достатній рівень захисту, але, зважаючи на швидкий розвиток техніки і математики, перспективи появи і використання квантових комп’ютерів, актуальною також залишається необхідність його розвитку. Стандарт обмежується максимальним степенем поля 509, у той час як міжнародним стандартом рекомендуються до використання поля в оптимальному нормальному базисі з степенем розширення основного поля до 998.За результатами аналізу формується уява про багаторівневу структуру операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. Верхній рівень забезпечує обмін інформацією із зовнішнім середовищем. Нижній (власне спеціалізований, СП) – забезпечує виконання специфічних для даного завдання операцій.

Одним з основних елементів для проєктування функціональних вузлів спеціалізованих комп’ютерів є ПЛІС, у яких останнім часом з’явилися такі важливі властивості.

1) ПЛІС полегшує наступний швидкий перехід до *ASIC,* тобто, до масового виробництва, апаратної реалізації алгоритмів та збереження всередині мікросхеми проміжних результатів при виконанні цих алгоритмів;

2) сучасні ПЛІС забезпечують збереження інтелектуальної власності та ускладнюють несанкціоноване тиражування та «зворотне проєктування».

На сучасному етапі, коли КЗІ впроваджуються у КФС, важливим стає забезпечення їх роботи у реальному масштабі часу. Це вимагає використання швидкодіючих апаратних рішень – спецпроцесорів, які реалізуються в програмовних логічних інтегральних схемах (ПЛІС). Як базу для проєктування засобів КЗІ взято багаторівневий спецпроцесора (СП), який при опрацюванні цифрових підписів виконує операції над точками еліптичних кривих. Проектування такого спецпроцесора вимагає використання спеціальних розділів математики: полів Галуа, еліптичних кривих (ЕК) тощо. Елементи полів Галуа та точки ЕК представляються за допомогою багаторозрядних двійкових кодів (розрядністю сотні і тисячі біт.

СП вимагає оригінальних засобів для виконання операцій над ними. СП функціонує на основі таких теоретичних положеннях, які дозволяють розглядати його як спеціалізовану комп’ютерну систему (СКС) з архітектурою, відмінною від відомих архітектур КЗ

Від сучасних комп’ютерних засобів вимагається дотримування принципів побудови відкритих систем, що орієнтує на використання відкритих стандартів.

В Україні діють декілька стандартів на ЕЦП: міждержавний стандарт ГОСТ 34.310-95 та орієнтований на використання еліптичних кривих національний стандарт України ДСТУ 4145-2002. Підтримку застосуванню ЕЦП надають стандарти, що забезпечують неспростовність ЕЦП, розкривають механізми роботи ЕЦП на основі ідентифікаторів та сертифікатів. Також стандартизовано методи роботи із еліптичними кривими ДСТУ ISO/IEC 15946-1: 2015, установлення ключів ДСТУ ISO/IEC 15946-3: 2008, оновлено процедури шифрування ДСТУ 7624:2014 і гешування ДСТУ 7564:2014.

Вирішення завдань захисту від несанкціонованого використання і від

пошкодження інформації відомі і широко використовується на практиці. Але сучасні методи, які базуються на використанні розширених полів Галуа *GF(pm),* де *p > 2,* та суперсингулярних еліптичних кривих і які здатні протистояти використанню квантових комп'ютерів з метою злому системи захисту, на сьогоднішній день розроблено недостатньо, особливо це стосується апаратних методів.

Вищесказане визначає актуальність створення методів і засобів проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. І в роботі пропонуються рішення цього завдання.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертація відповідає науковому напряму кафедри електронних обчислювальних машин: "Питання теорії, проєктування та реалізації комп'ютерних систем та мереж, а також комп'ютерних засобів, вузлів, приладів і пристроїв вимірювальних, інформаційних, керуючих телекомунікаційних та кіберфізичних систем" та виконувалась в межах держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446).

**Мета і задачі дослідження.** Метою дисертаційної роботи є наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

Для досягнення поставленої мети слід вирішити задачі:

провести системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП);

визначити основні архітектурні принципи побудови та розробити узагальнену модель операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розробити метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ та метод оцінювання складності злому апаратних засобів КЗІ;

вдосконалити метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі;

вдосконалити метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розробити технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розробити уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

провести експериментальне дослідження та впровадження розроблених операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

**Об'єкт дослідження** – операційні вузли для полів Галуа, які використовуються при КЗІ на основі ЕК.

**Предмет дослідження** – методи та засоби структурної організації операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, методи та засоби проєктування, порівняння, синтезу та маскування роботи таких пристроїв.

**Методи дослідження.** При проєктуванні операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК враховувалися висновки теорії обчислювальних машин, теорії обчислювальних систем, теорії комп'ютерних систем, теорії проєктування спеціалізованих комп'ютерних систем. Для реалізації елементів операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК на ПЛІС використовувалися висновки теорії проєктування НВІС, теорія алгоритмів, теорія цифрових автоматів. Для розроблення методів опрацювання елементів полів Галуа та точок еліптичних кривих враховувалися положення і висновки теорії чисел, теорії залишків, теорії обчислень, теорії груп, теорії інформації, для проєктування спецпроцесорів застосовувалися результати теорії кодування, для створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК та для дослідження їх роботи були задіяні теорія моделей,

теорія програмування, обчислювальна математика, моделювання алгоритмів та апаратних засобів.

Перевіряння отриманих результатів здійснювалося відповідно до теорії випробовувань шляхом моделювання.

Виконані дослідження використовують результати, отримані з прикладної теорії цифрових автоматів стосовно структурного синтезу й логічного проєктування цифрових пристроїв, з теоретичної моделі взаємозв'язку відкритих систем. Також використано і розвинуто: комп'ютерні методи виконання математичних операцій у простих та розширених полях Галуа у поліноміальному базисі, комп'ютерні методи виконання операцій над точками еліптичних кривих. У проведених дослідженнях широко використовується математичний апарат теорії алгоритмів, апарат теорії чисел, а також засоби моделювання цифрових схем.

**Наукова новизна** одержаних результатів.

На основі проведених досліджень здійснено наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів, розв'язано важливе наукове завдання створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які працюють з елементами розширених полів Галуа $GF(p^m)$, розроблено структурні алгоритми їх роботи. При цьому розв'язано такі взаємозв'язані задачі і отримано такі нові наукові результати:

вперше запропоновано метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$, який базується на представленні помножувача для поліноміального базису як матриці модифікованих комірок Гілда і дозволяє визначити поля Галуа $GF(p^n)$ з приблизно однаковим порядком, у яких моделі будуть мати найменше значення складності (часової, ємнісної, структурної, програмної, а також апаратної);

вперше запропоновано метод оцінювання складності злому апаратних засобів КЗІ, у якому прийнято, що засоби КЗІ реалізовано апаратно, а засоби злому –

програмно, і який дозволяє визначити поля Галуа $GF(p^m)$ з приблизно однаковим порядком, у яких злом засобів КЗІ буде виконуватися найдовше;

вперше запропоновано метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі, який полягає у використанні незалежних від значення операндів алгоритмів знаходження обернених елементів і який дозволяє зменшити витоки інформації із засобів КЗІ сторонніми каналами;

отримав подальший розвиток метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, який, на відміну від відомих методів, полягає у введенні до моделі вузла детектора заборонених значень окремих розрядів кодів елементів полів Галуа, що дає можливість виявляти частину апаратних помилок;

**Практичне значення одержаних результатів**. Отримані у дисертаційній роботі наукові результати створюють методологічну базу для розроблення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ.

Практична цінність дисертаційної роботи полягає у тому, що за результатами теоретичних та експериментальних досліджень для конфігуровних операційних пристроїв, які опрацьовують елементи розширених полів Галуа:

створено і апробовано технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

створено та перевірено уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

визначено найкращі для використання розширені поля Галуа, за сукупністю показників найращим є розширене поле з характеристикою 3.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання,

автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом) (Додаток А, Додаток Б).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»), що підтверджено відповідним Актом (Додаток В).

**Особистий внесок здобувача.** Усі основні положення, що становлять суть дисертації, отримано автором самостійно і повністю розкрито у публікаціях. У публікаціях, що написано в співавторстві, автору дисертації належать основні теоретичні та практичні результати (методи і підходи до рішення поставлених задач). Зокрема, [21], [44], [70], [155] – запропоновано модель помножувача елементів розширених полів Галуа для визначення його часової складності та метод її визначення, проведено дослідження та аналітичне опрацювання та узагальнення їхніх результатів; [75], [45], [71], [152] – запропоновано модель модифікованої комірки Гілда та помножувача елементів полів Галуа на її основі у поліноміальному базисі для визначення структурної складності помножувача та метод її визначення, проведено дослідження та аналітичне опрацювання й узагальнення їхніх результатів; [153] – запропоновано алгоритми знаходження обернених елементів полів Галуа у поліноміальному базисі, моделі вузлів та VHDL-описи, які реалізують дані алгоритми з різними типами помножувачів елементів полів Галуа, які характеризуються незалежним від кодів операндів часом обчислення; [156] - теоретичне обґрунтування можливості вирівнювання часу обчислення обернених елементів у поліноміальному базисі двійкових розширених полів Галуа на основі біт-паралельних помножувачів, моделі пристроїв та методи їх використання для обчислення обернених елементів; [157] – запропоновано метод оцінювання часової

складності помножувачів елементів розширених полів Галуа на універсальних комп’ютерах і графічних процесорах з врахуванням виконання ними векторних операцій; [158] - запропоновано метод оцінювання часової складності засобів КЗІ при їхній апаратній реалізації та використанні для злому універсальних комп’ютерів (програмної реалізації злому); [159] - запропоновано метод визначення ефективності апаратних реалізацій алгоритмів постквантової криптографії на основі еліптичних кривих, проведено дослідження та аналітичне опрацювання й узагальнення їхніх результатів; [43], [73] – визначено розширені поля Галуа, які є найбільш тестопридатними для організації вбудованого контролю операційних вузлів та вдосконалено метод формування ознаки збою.

**Апробація результатів дисертації.** Основні положення та результати роботи доповідалися і обговорювалися на таких наукових конференціях та семінарах:

V Міжнародний молодіжний науковий форум “Litteris et Artibus”. 26–28 листопада, 2015. Україна, Львів;

International Youth Science Forum ”Litteris et Artibus”, November 24-26, 2016, Lviv, Ukraine;

International Youth Science Forum ”Litteris et Artibus”, November 23-25, 2017, Lviv, Ukraine;

2-а Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика (Елтекс 2016)», м. Одеса, 26–28 червня 2016 р.;

Другий науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р.;

Третій науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 13-14 червня 2017 р.;

Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика (ЕЛТЕКС-2017). Одеса, Одеський національний політехнічний університет. 26 – 28 червня 2017 р.;

4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International

Conference ICTERI2018). May 14, 2018, Kyiv;

9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT'2018. Kyiv, May 24-27;

Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика ЕЛТЕКС – 2018, м. Одеса, Одеський національний політехнічний університет. 29 травня – 1 червня 2018 року;

International Conference "Advanced Computer Information Technologies", June 1-3, 2018 in Ceske Budejovice, Czech Republic.

**Публікації.** Основні положення дисертаційної роботи висвітлені у 16 наукових публікаціях, з яких : 1 колективна монографія: 2 статті у наукових фахових виданнях України, які включено до міжнародної науково-метричної бази РІНЦ, 4 статті у наукових фахових виданнях України, 8 матеріалів наукових конференцій та семінарів.

**Структура та обсяг роботи.** Дисертаційна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Роботу викладено на 189 сторінках, з них сторінок основного тексту - 134. Робота містить рисунків - 42, таблиць - 32, додатків - 16. Найменувань у списку використаних джерел - 209.

# РОЗДІЛ 1
# АНАЛІЗ ЗАГАЛЬНИХ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЄКТУВАННЯ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

У цій дисертаційній роботі виконується наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів. Для досягнення поставленої мети важливим є системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП). Далі у цьому розділі виділені базові положення, на яких при цьому повинна бути зосереджена увага.

## 1.1. Кіберфізичні системи

Упродовж останніх кількох років спостерігається підвищена активність в сфері створення та застосування кіберфізичних систем (КФС). Під КФС розуміють поєднання фізичних процесів та кібернетичних компонентів [60], які забезпечують організацію вимірювально-обчислювальних процесів, захищене зберігання та обмін вимірювальною і службовою інформацією, організацію та здійснення впливів на фізичні процеси. Об'єднання компонентів КФС у межах єдиної бездротової системи дає змогу отримувати якісно нові результати, які можна використовувати для створення широкого спектра принципово нових наукових, технічних та сервісних засобів, але одночасно ставить підвищені вимоги до КЗІ всередині системи.

Застосування КФС розглядається [38] у контексті:

1) створення інтелектуального виробництва, інтелектуального енергопостачання, інтелектуальних споруд, інтелектуального транспорту, інтелектуальних систем оборони;

2) формування Інтернет речей як мережі фізичних об'єктів з вбудованими давачами для реєстрації та передавання даних про стан різнорідних об'єктів,

середовища та структури взаємодії “об’єкт – середовище”.

1.2. Криптографічний захист інформації кіберфізичних систем

Засоби КЗІ є важливою складовою КФС. До цих засобів належать шифропроцесори, які здійснюють опрацювання цифрових підписів, використовуються для побудови криптографічних систем з відкритим ключем, реалізують протоколи захисту даних симетричними блоковими шифрами в локальних комп'ютерних мережах, а також засоби визначення стійкості до вторгнень, виявлення атак і доступу до інформації.

Як показано в [209] частка обладнання однієї з різновидів КФС, Інтернету речей, яке використовує КЗІ, стає все меншою (Додаток Р, Рис. Р. 1). Це гостро ставить задачу забезпечення кібербезпеки (Додаток Р, Рис. Р. 2), найвищий пріоритет – 87,8 % [193]), розробки і впровадження нових і ефективних методів та засобів КЗІ.

**1.2.1.** Методи захисту КФС.

Найважливішими ознаками комп’ютерних систем спеціального призначення є жорсткі умови експлуатації та захищеність інформації у каналах зв’язку, що стає надзвичайно важливим у зв’язку із постійним збільшенням кількості атак на КС, а останнім часом і на КФС [83, 86] та вбудовані КС [24].

**Методи забезпечення інформаційної безпеки.** Загальні методи забезпечення інформаційної безпеки поділяються на криптографічні, технічні, правові, організаційні та економічні. Серед задач КЗІ є задача розроблення, використання і вдосконалення засобів опрацювання цифрових підписів, яке передбачає використання операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК [179] і методів контролю ефективності цих засобів, забезпечення їхньої роботи у реальному часі.

1.2.2. **Типи комп’ютерних засобів КЗІ.** Для побудови комп’ютерних засобів КЗІ використовують три види засобів: 1) програмні (універсальний процесор з програмою, яка завантажується), 2) програмно-апаратні (універсальний процесор з прошитою незмінною програмою); 3) апаратні (цифровий автомат, СП). Їх основна відмінність полягає 1) в способі виконання покладених на них функцій; 2) в ступені

надійності реалізованих методів; 3) в ціні, що часто стає для користувачів визначальним чинником. Як правило, дешеве рішення - програмне, дорожче - апаратне. Вища вартість апаратних пристроїв окупається вищою якістю захисту інформації.

1.2.3. **Алгоритм.** Під алгоритмом розуміють точний наказ, що веде від варійованих початкових даних до шуканого результату [107]. Поняття алгоритму в математиці є первісним, таким, як множина, число і т.д., тому його не можна точно означити .

1.2.4. **Повна побудова алгоритму.** Теоретична і практична діяльність з використанням комп'ютерів вимагає здійснення повної побудови алгоритму [34]: 1) формулювання задачі; 2) побудови моделі (абстрактного алгоритму); 3) розроблення алгоритму (абстрактного); 4) перевіряння правильності алгоритму (абстрактного); 5) реалізації алгоритму (структурного); 6) аналізу алгоритму і його складності; 7) перевіряння реалізації (структурного алгоритму); 8) оформлення документації.

1.2.5. **Абстрактні цифрові автомати і абстрактні алгоритми.** Методи теорії цифрових автоматів [77] використовуються для проєктування як апаратного так і програмного [115] забезпечення комп'ютерів.

1.2.6. **Структурний цифровий автомат і структурні алгоритми.** Структурний автомат на відміну від абстрактного має декілька елементарних вхідних $n$ та вихідних $m$ каналів. Канонічний метод структурного синтезу цифрового автомата можна умовно розділити на наступні етапи [77]: 1) кодування; 2) вибір елементів пам'яті автомата; 3) вибір структурно-повної системи елементів; 4) побудова рівнянь булевих функцій виходів і збудження автомата; 5) побудова функціональної схеми автомата.

1.2.7. ***SH*-модель алгоритму, складність алгоритму.** Для прикладних досліджень складності універсальних алгоритмічних систем обчислень потрібні моделі, які б об'єднали здобутки теорії абстрактних алгоритмів з практикою проєктування і розв'язання задач на реальних комп'ютерах. Такою моделлю може бути програмно-апаратна *SH*-модель алгоритму [80], [81].

1.2.8. **Апаратна реалізації алгоритмів**

При апаратній реалізації алгоритмів захищеність інформації забезпечується

спеціальною апаратурою – спеціалізованими операційними вузлами, які разом утворюють спецпроцесор (СП, для засобів КЗІ – шифропроцесор (ШП) або криптопроцесор (КП)) [24].

***До переваг апаратної реалізації*** належать [87]: 1) кращі швидкісні характеристики; 2) більша фізична захищеність від побічних електромагнітних випромінювань і від безпосереднього фізичного впливу на пристрій, у якому здійснюється захист інформації та збереження ключової інформації; 3) зменшення споживаної потужності; 4) більша зручність в експлуатації, операції виконуються у прозорому для користувача режимі; 5) полегшена інсталяція [175].

Також перевагами апаратних реалізацій є: 1) гарантія незмінності алгоритму шифрування; 2) наявність апаратного давача випадкових чисел (ДВЧ), який застосовується при генерації ключів; 3) можливість прямого (без використання системної шини комп'ютера) завантаження ключів шифрування в СП з персональних носіїв; 4) зберігання ключів шифрування в пам'яті СП; 5) ідентифікація і аутентифікація користувача до завантаження операційної системи; 6) заборона на зміну процесу завантаження комп'ютера; 7) можливості контролю цілісності операційної системи і прикладного програмного забезпечення; 8) ведення доступного лише адміністраторові безпеки журналу дій користувачів; 9) забезпечення зіставної з програмними продуктами швидкості шифрування.

Обмеженість часу на опрацювання інформації та зменшена продуктивність КФС в порівнянні з ПК також вимагає апаратної реалізації алгоритмів. Основним недоліком апаратної реалізації є наявність програмного інтерфейсу.

У даній дисертаційній роботі здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

### 1.3. Розвиток теорії та практики захисту інформації у КФС.

Основи теорії для створення КФС розроблено в роботах А. О. Мельника [60].

В основі процедур отримання і перевіряння ЕЦП відповідно до [93] лежать

операції над елементами поля Галуа $GF(2^m)$ і точками ЕК. Великий внесок у впровадження теорії полів Галуа у практичні розробки зробив Николайчук Я. М. [64], [65], [66], [67], [180], значну увагу виконанню операцій над елементами полів Галуа та точками еліптичних кривих, а також практичним аспектам визначення складності комп'ютерних систем висвітлено у роботах В. С. Глухова [6], [7], [8], [9], [10], [12], [13], [14], [15], [16], [17], [18], [25].

Важливо відмітити внесок в теорію і практику КЗІ, який зробили розробники Державних стандартів України А. І. Кочубінський [53] та О. С. Шаталов [93], А. Анісімов [95], [97], М. Карнаух [96], І. Горбенко, Г. Гулак, О. В. Потій, Л. Ковальчук, Д. Шевченко, Д. Балагура, А. Лєншин, Ю. Горбенко та І. Остапенко [98], [99]. Теоретичним і практичним аспектам проєктування засобів КЗІ присвячено роботи А. О. Мельника [51], [59, [52], В. М. Ємця [46], [51], Р. Б. Поповича [46], В. А. Мельника [46], [51], О. В. Потія [55], [30], [68], І. Д. Горбенка [29], [30], [4], [82]. Математичні основи криптографії викладено у [56], основні питання коротко викладено у енциклопедичному виданні [188]. Питання системності КЗІ розробляє В. В. Домарев [37]. Велике значення при проєктуванні засобів КЗІ має їхня порівняльна оцінка, так саме, як і оцінка складності алгоритмів, які реалізують ці засоби. Програмно-апаратну модель алгоритмів і теорію складності на її основі розробив М. В. Черкаський [80], [81].

## 1.4. Криптографія еліптичних кривих

В Україні використання операцій над елементами полів Галуа регулюється стандартами опрацювання цифрових підписів ДСТУ 4145-2002 [93] та ДСТУ ISO/IEC 15946-1: 2015 [98], в основу яких покладено операції над точками несингулярних еліптичних кривих у полі Галуа GF(2m). Популярність цього математичного апарату обумовлена можливістю застосовування відносно невеликої довжини ключа і блоку перетворень по відношенню до інших алгоритмів. Це дає змогу при однакових апаратних витратах на реалізацію пристрою збільшити надійність цифрового підпису. Тому актуальним залишається питання мінімізації обчислювальної, апаратної, часової, структурної та програмної складностей. Хоча на сьогоднішній день стандарт дозволяє забезпечити більш ніж достатній рівень

захисту, але, зважаючи на швидкий розвиток техніки і математики, перспективи появи і використання квантових комп'ютерів, актуальною також залишається необхідність його розвитку. Стандарт обмежується максимальним степенем поля 509, у той час як міжнародним стандартом [191] рекомендуються до використання поля в оптимальному нормальному базисі з степенем розширення основного поля до 998.

1.4.1. **Стандарти для систем ЕЦП.** На засоби опрацювання цифрових підписів накладаються такі самі вимоги та обмеження, як і на КС в цілому – застосування принципів побудови відкритих систем [94], що складаються з апаратних і програмних продуктів і технологій, розроблених відповідно до загальнодоступних і загальноприйнятих (міжнародних) стандартів.

В Україні діють декілька стандартів на ЕЦП: міждержавний стандарт ГОСТ 34.310-95 [89] та орієнтований на використання еліптичних кривих національний стандарт України ДСТУ 4145-2002 [93, Додаток О]. Підтримку застосуванню ЕЦП надають стандарти, що забезпечують неспростовність ЕЦП [96], розкривають механізми роботи ЕЦП на основі ідентифікаторів та сертифікатів [97]. Також стандартизовано методи роботи із еліптичними кривими ДСТУ ISO/IEC 15946-1: 2015 [100]), установлення ключів ДСТУ ISO/IEC 15946-3: 2008 [99], оновлено процедури шифрування ДСТУ 7624:2014 [98] і гешування ДСТУ 7564:2014 [101]).

Для практичної реалізації [154], [158] корисними є рекомендації та вимоги міжнародних стандартів [191], які передбачають використання розширених двійкових полів Галуа $GF(2_m)$ із степенем $m \leq 998$. Український стандарт на ЕЦП [93] обмежується використання полів Галуа із степенем $m \leq 509$. У даній роботі розробляються перспективні засоби і методи опрацювання елементів полів Галуа. При цьому поля відповідають вимогам українських стандартів, мають степінь, який відповідає вимогам міжнародних стандартів, та можуть бути використані при проєктуванні постквантових засобів КЗІ, у чому і полягає актуальність даної роботи.

При використанні персональних комп'ютерів, в електронній комерції турбота про захищеність даних стала завжди необхідною. Раніше розробники вбудованих і

спеціалізованих КЗ відчували себе більш вільними стосовно захисту своїх даних. Але зараз вбудовані засоби об’єднуються в КФС з використанням таких комунікаційних відкритих каналів як *Ethernet*, *Wi-Fi*, *Bluetooth*, або *RFID*, і питання захисту інформації КФС стає першочерговим [163].

Сучасні методи КЗІ можна поділити на чотири крупні класи [2]: 1) симетричні, 2) з відкритим ключем, 3) системи ЕЦП, 4) системи керування ключами. Основні напрями використання цих методів : 1) передача конфіденційної інформації каналами зв'язку, 2) зберігання інформації на носіях в зашифрованому вигляді, 3) встановлення достовірності повідомлень, що передаються.

1.4.2. Принципи використання електронного цифрового підпису

ЕЦП побудований на принципах асиметрії – для генерації підпису використовується «секретний» ключ, відомий тільки автору підпису, а для перевіряння підпису використовується «відкритий» ключ [2]. Обидва ключі підпису математично пов'язані між собою так, що знаючи відкритий ключ підпису неможливо визначити секретний ключ.

ЕЦП виробляється за допомогою математичних операцій у полях Галуа, з використанням алгоритму гешування (стиску) повідомлення. Неможливість підробки підпису забезпечується властивостями поля, у якому проводяться обчислення, а саме, трудомісткістю розв’язання задачі дискретного логарифмування в цьому полі, а також трудомісткістю створення заданої геш-функції. Принципи утворення і перевіряння ЕЦП – див. Додаток Д.

Учасники обміну даними потребують захисту від безлічі зловмисних дій, до яких відносяться: 1) відмова; 2) фальсифікація; 3) зміна.

Встановлення достовірності і верифікація повідомлення мають схожі елементи: ЕЦП є посвідченням достовірності інформації з додаванням вимоги про її залежність від змісту повідомлення. Відомі підсистем ЕЦП, у яких виникає необхідність забезпечення інформаційної безпеки в умовах взаємної недовіри чи змови учасників протоколу. Одним з найважливіших етапів створення таких підсистем є вибір алгоритму ЕЦП. Загальна концепція та теоретичні основи методології проєктування алгоритмів ЕЦП наведені у [1].

1.4.3. **Еліптичні криві і спеціалізовані обчислювачі.** Огляд історії [2] та основних операцій при опрацюванні цифрових підписів на основі ЕК містить Додаток Е. Особливості роботи з еліптичними кривими викладено в стандартах [98], [99], [196], [199] короткі відомості про Державні стандарти України містить Додаток О.

Як видно (Додаток О), для опрацювання цифрових підписів необхідно виконувати додавання точок еліптичних кривих і множення точки еліптичної кривої на ціле число. Остання операція зводиться до послідовності операцій додавання точок. Для виконання додавання точок необхідно виконати операції множення і ділення елементів полів Галуа, тому прискорення множення елементів полів Галуа є актуальною і важливою задачею (ділення зводиться до послідовного виконання кількох операцій множення).

ЕК можуть бути визначені над простими скінченими полями $GF(p)$ і над розширеними полями Галуа $GF(p^n)$ ($p$ – просте число, $n$ – натуральне число) [2]. У полях $GF(2^n)$ обчислення прискорюються, особливо при наявності спеціалізованого апаратного обчислювача, на який найчастіше покладається обчислення найскладніших операцій – множення і ділення елементів обраного поля Галуа.

Число ЕК з потрібними властивостями над розширеними двійковими полями дуже невелике. Це практично не дозволяє користувачу вибрати криву за своїм розсудом, що трохи підриває довіру до цих кривих.

1.4.4. **Стійкість стандартів електронного цифрового підпису.** Стійкість стандартів ЕЦП [191], [93] заснована на складності розв’язання задачі дискретного логарифмування в групі точок ЕК.

Найбільш швидкими алгоритмами розв’язання задачі дискретного логарифмування в групі точок ЕК при правильному виборі параметрів вважаються $\rho$-метод і $\lambda$-метод Полларда [121]. Для поліпшеного $\rho$-методу Полларда обчислювальна складність оцінюється для кобліцевих кривих над полями $GF(2^p)$ як $I_p = \sqrt{\pi n / 4p}$ і для усіх інших кривих над полями $GF(2^p)$ і $GF(p)$ як $I_p = \sqrt{\pi n / 4}$ [186]. У всіх випадках обчислювальна складність визначає кількість операцій додавання точок ЕК.

З результатів робіт [163] можна оцінити обчислювальну складність $I_p$ розв'язку задач дискретного логарифмування в групі точок ЕК (кількість операцій додавання точок ЕК) і складність $I_{pp}$ розв'язку задач дискретного логарифмування у простому полі (кількість операцій множення елементів у полі *GF(p))*. Алгоритми ЕЦП, що ґрунтуються на ЕК, забезпечують більшу захищеність інформації приблизно в $10^{n/10}$ разів, де $n$ – довжина ключа. Порядок $10^{26}$ недосяжний для сучасних класичних комп'ютерів. Але, по-перше, схема ЕЦП повинна гарантувати достатній рівень захисту на роки вперед. По-друге, є прецедент [207] розв'язання задачі факторизації 512-бітового числа. Складність дискретного логарифмування лише в константу разів вище. І вже з'являються квантові комп'ютери.

1.4.5. Стійкість засобів криптографічного захисту інформації

Стійкість засобів КЗІ вимірюється в умовних одиницях, які представляють двійковий логарифм від приблизної обчислювальної потужності $R$ (необхідної для простої криптографічної операції, наприклад, одноразової оцінки блочного шифру на одному блоці) для обчислення дискретних логарифмів в еліптичних кривих (ECDLP) та / або факторизації чисел заданої довжини бітів [185] (Додаток Н, Таблиця Н. 3).

Таблиця Н. 1 (Додаток Н) [36] містить порівняння рекомендацій щодо довжини ключа для ECDSA, яка повинна забезпечувати достатню криптографічну стійкість. Простежується закономірність, що чим раніше були розроблені рекомендації, тим меншу мінімальну довжину ключа вони пропонують на майбутні роки. Це дозволяє зробити висновок, що розмір ключа втрачає свою криптографічну стійкість раніше, ніж це передбачається. Рекомендовані довжини ключів містить Таблиця Н. 2 [194]. Тому актуальною стає задача проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК на основі еліптичних кривих для полів, порядок яких перевищує межі, встановлені стандартом [93].

1.5. Технології квантових обчислень і криптографічний захист інформації

1.5.1. Методи постаквантової криптографії

З розвитком технологій квантових обчислень і появою квантового комп'ютера виникає загроза поточному стану захищеності криптографічних систем з відкритим

ключем [136]. З появою квантового комп'ютера, який буде мати необхідний для методів квантового криптоаналізу об'єм регістру розподілених квантів, стійкість існуючих криптоалгоритмів значно знизиться [172], [122]. З цього випливає необхідність створення алгоритмів стійких до методів квантового криптоаналізу [31], [32], [68]. Європейський проєкт «Нові європейські алгоритми для електронного підпису, цілісності та шифрування» (NESSIE) та Національний інститут стандартів і технологій (NIST) США об'явили про початок набору претендентів на конкурс постквантових алгоритмів, стандарти щодо яких планується прийняти в 2020–2022 роках [144], [*200*].

В [136] відмічається, що в серпні 2015 року агентство національної безпеки (АНБ) уряду США виступило з великою заявою про необхідність розробки стандартів пост квантової криптографії. В цій статті проаналізовано небезпеку для сучасних криптоалгоритмів у випадку застосування квантових комп'ютерів та запропоновано механізми криптоперетворень, що є стійкими до квантового криптоаналізу різних типів (Таблиця 2.9).

Безпека сучасних інформаційних систем та технологій базується на стійкості криптографічних перетворень, які вони використовують для криптографічної обробки інформації [29]. З використанням квантового алгоритму Шора [172] складність криптоаналізу таких криптосистем як RSA, DSA, ECC (криптографії з використанням еліптичних кривих) за допомогою квантових комп'ютерів буде поліноміальною (що припускає розв'язання задачі злому системи), хоча з використанням класичних алгоритмів криптоаналізу, відомих на сьогодні, складність атаки на такі криптосистеми є субекспоненційною або експоненційною.

Для забезпечення криптографічної стійкості перетворень у групі точок не сингулярних еліптичних кривих, бо саме таке перетворення використовується в національному стандарті [93], у перспективі необхідно збільшувати розміри загальних параметрів з порядком базової точки навіть до 1024 бітів, що більше ніж визначено національним стандартом [93] і міжнародним стандартом [191]. Тобто, розміри загальносистемних параметрів криптосистеми на базі еліптичних кривих можна підняти аж до 1024 біт, тоді квантовий комп'ютер повинен мати 7218-

кубітний процесор для зламу такої криптосистеми [29] (на сьогоднішній день відомі квантові комп'ютери, які мають 51 кубітний процесор [112], але сучасні ПЛІС дозволяють вже зараз побудувати цифрові квантові комп'ютери з сотнями кубіт в одній ПЛІС [128], [129], [130]).

Можна виділити такі класи криптосистем, що будуть стійкими до квантового криптоаналізу [114], [208]: • Криптографія на основі решіток. • Мультиваріативна криптографія. • Криптографія на основі ґеш-функцій. • Криптографія на основі кодів. • Симетрична криптографія. • Криптографія ізогеній суперсингулярних еліптичних кривих (що підштовхує до продовження досліджень за темою даної дисертаційної роботи).

1.5.2. Криптографія ізогеній суперсингулярних еліптичних кривих

Криптографія, яка заснована на ізогенії, передбачає використання полів Галуа з великими характеристиками (наприклад, $d \approx 2^{768}$) і становить цікаву альтернативу наведеним вище напрямкам постквантової криптографії [116]. Це пояснюється тим, що вона базується на природній обчислювальній проблемі теорії чисел, а саме на проблемі обрахунку ізогенезису між еліптичними кривими. Ці системи можна віднести до одного з напрямків постквантової криптографії, такі системи базуються на теоретико-числовому припущенні. Враховуючи те, що національний стандарт [93] вироблення та перевірки цифрового підпису базується на еліптичних кривих, то такий напрямок є надзвичайно важливим і перспективним для використання в Україні [29]. В роботі [117] наведено аналітичні показники стійкості такої криптосистеми, де показано, що складність криптоаналізу такої криптосистеми з використанням класичних комп'ютерів складає $O(\sqrt[4]{p})$, для квантових комп'ютерів $O(\sqrt[6]{p})$.

1.6. Поля Галуа як математична основа електронних цифрових підписів

1.6.1. Початкові поняття та визначення. Початкові математичні поняття та визначення, які стосуються використання електронних цифрових підписів містить Додаток Ж.

Основою є теорія груп, поля Галуа, ЕК [125], [3] та інші спеціальні розділи

математики. Ці розділи систематизовано викладено в багатьох роботах [5], [141], [191], [164], [79]. Процесори та їх елементи в кодах поля Галуа розглянути в [64].

1.6.2. Під час виконання операцій над елементами поля Галуа, представленими у нормальному базисі, доводиться виконувати операції над матрицями. Алгоритми виконання цих операцій відомі [35].

Також відомі апаратні та програмні реалізації цих алгоритмів [7].

1.6.3. Представлення елементів полів Галуа у засобах криптографічного захисту інформації

Елементи $\{t^{m-1},...,t^2,t,1\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\{\theta,\theta^2,\theta^{2^2},...,\theta^{2^{m-1}}\}$ 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). У будь-якому варіанті елементи розширених полів Галуа $GF(d^m)$ представляються у засобах КЗІ у вигляді рядка символів $a_{m-1}a_{m-2}\ldots a_1a_0$ (у поліноміальному базисі) або $a_0a_1\ldots a_{m-2}a_{m-1}$ (у нормальному базисі) (рис. 2.2).

Піднесення до квадрату у нормальному базисі зводиться до циклічного зсуву операнда, що обумовлює широке використання нормального базису в криптографічних алгоритмах, які вимагають знаходження обернених елементів шляхом виконання послідовності операцій множення та піднесення до степеню [146].

1.6.4. **Операції над елементами простих полів Галуа *GF(n).*** Однією з операцій опрацювання ЕЦП є модульне додавання та множення ($s = (e + dr) \bmod n$). Складність виконання цих операцій визначається великою розрядністю операндів та необхідністю порівняння проміжних результатів з модулем *n.* Відомий метод Монтгомері, який полягає у виконанні вказаних операцій за модулем $N>n$, із зведенням всіх проміжних результатів *r* більших або рівних *N* за модулем *n. N* вибирають зручним для аналізу умови $r<N$. Недоліками методу є низька швидкодія довгих комбіна-

ційних схем додавання, необхідного для зведення за модулем $n$, невизначеність часу обчислення (для різних проміжних результатів можливо від 0 до 4 зведень за модулем $n$).

1.6.5. Поля Галуа, що використовуються у засобах КЗІ

На сьогоднішній день стандартизовано використання двійкових полів Галуа $GF(2^m)$ для опрацювання електронних цифрових підписів [93]. 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 $p = 3$ [98]. Для постквантової криптографії зараз аналізується використання поля із характеристикою $p \approx 2^{768}$ [117].

Тому в роботі розглядаються

двійкові поля Галуа $GF(2^m)$, оскільки зараз вони практично використовуються,

трійкові поля $GF(3^m)$ – для використання в найближчому майбутньому,

інші поля $GF(p^m)$ з великими характеристиками $p$, які, передбачається, буде задіяно у постквантовій криптографії.

1.7. Складність пристроїв опрацювання елементів полів Галуа

В процесах синтезу, аналізу і оптимізації SH-моделей пропонується використовувати п’ять характеристик складності: апаратну, часову, ємнісну, програмну і структурну [80], [81], які зв’язані одна з одною і залежать одна від одної. У дисертаційній роботі увага зосереджена на аналізі і мінімізації усіх згаданих характеристик складності (крім програмної) та їх комбінацій, при цьому приймається, що програмна характеристика має допустиму для рішення поставлених задач величину.

У даний час математичною основою опрацювання цифрового підпису є еліптичні криві [93]. При цьому опрацювання точок еліптичної кривої базується на виконанні операцій у полях Галуа $GF(2^n)$, елементи яких можуть бути представлені у поліноміальному та нормальному базисах. Апаратна реалізація помножувача для таких полів вимагає великих витрат обладнання, але дає виграш у часі в порівнянні з програмною: Таблиця 1.2 містить результати для поліноміального базису [126].

У роботі [9] показано, що апаратне множення в поліноміальному і

нормальному базисах вимагає приблизно однакових апаратних і часових витрат, програмно множення у поліноміальному базисі виконується на 1-2 порядки швидше (Таблиця 1.1). Але недоліком поліноміального базису є залежність часу обчислення обернених елементів полів Галуа (такого елемента $b$, що $ab$=1, якщо $a\neq0$ – заданий елемент) від значення операндів ($a$) [9], ще демаскує роботу засобів КЗІ. Методи обчислення оберненого елемента у поліноміальному та нормальному базисах містить Додаток И.

Помножувачі можуть бути паралельними (в тому числі, на основі комірок Гілда [123]), послідовними і паралельно-послідовними - секційними. Для нормального базису апаратна складність помножувачів дозволяє проводити їхню реалізацію на сучасних ПЛІС. Але при великих значеннях степенів поля та кількості секцій неможливо реалізувати такі помножувачі через їх високу структурну складність [20], методи та результати оцінювання структурної складності окремого помножувача наведено в [18], багатосекційних помножувачів – у [26], оцінювання, що базується на використанні програмно-апаратної моделі – у роботах [84, 85], у [28] показано, що структурна складність помножувача для нормального базису поля Галуа $GF(2^m)$ лежить в межах від $(1/2 \ldots 3/4)m^2$. Розроблення методів оцінювання структурної складності дозволили розробити методи її зменшення [27].

З-за високої структурної складності помножувачів для нормального базису, що ускладнює їхню реалізацію на ПЛІС, у вагу в даній роботі сконцентровано на операційних пристроях для поліноміального базису.

*Таблиця 1.1*

**Порівняння часу виконання множення програмним способом**

| Спосіб множення | Час виконання, % |
|---|---|
| Елементи представлено у поліноміальному базисі, множення здійснюється у поліноміальному базисі | 100 |
| Елементи представлено у нормальному базисі, множення здійснюється у поліноміальному базисі | 240 |
| Елементи представлено у нормальному базисі, множення у здійснюється нормальному базисі | 4500 |

Перевага нормального базису проявляється при знаходженні оберненого елемента (такого елемента $b$, що $ab$=1, якщо $a\neq0$ – заданий елемент). Методи обчислення оберненого елемента у поліноміальному та нормальному базисах

містить Додаток И.

*Таблиця 1.2*

**Порівняння апаратної і програмної реалізацій**

| Operation over GF($2^{191}$) | Time in $\mu$sec | | Speed-up |
|---|---|---|---|
| | Software | GF Coprocessor | |
| Addition | 0.6 | 0.03 | 20.00 |
| Multiplication | 39.0 | 2.41 | 16.18 |
| Inversion | 126.0 | 4.81 | 26.20 |
| EC Addition | 215.0 | 24.61 | 8.74 |
| EC Doubling | 220.0 | 27.05 | 8.13 |

Одним з можливих варіантів розв'язку задачі зменшення апаратної та структурної складності є перехід до використання полів Галуа з характеристикою $p$, більшою ніж 2, в першу чергу – з характеристикою 3 [49]. У роботах [47, 48] запропоновано метод оцінювання апаратної складності помножувачів для розширених полів Галуа і показано, що за апаратною складністю трійкові поля у поліноміальному базисі мають перевагу перед двійковими. Поля з більшими характеристиками ($p > 3$) не аналізувалися.

1.8. Особливості архітектури засобів КЗІ

1.8.1. **Типи операційних пристроїв спеціалізованих комп'ютерів.** Залежно від принципів побудови можна провести наступну класифікацію операційних пристроїв [58]: 1) табличні операційні пристрої; 2) алгоритмічні операційні пристрої; 3) таблично-алгоритмічні операційні пристрої.

**Багаторівневі структури у комп'ютерних системах.** Багаторівневі структури широко використовуються в КС для збільшення продуктивності та кількості задач, що одночасно розв'язуються. Відомі дворівневі [59] та багаторівневі системи захисту інформації [33], багаторівнева організація комп'ютера [54] та його пам'яті [58], ієрархічні рівні багаторівневої структури [69], багаторівневі структури систем автоматизації [184].

1.8.2. **Еталонна модель взаємозв'язку відкритих систем.** Для побудови відкритих систем використовується багаторівнева модель їхнього взаємозв'язку. Найбільш структуровано принцип побудови багаторівневих систем викладено у [94], [92], де наведено базову семирівневу еталонну модель взаємозв'язку відкритих сис-

тем. При обміні даними між сумісними рівнями …, *N*+1, *N*, *N*-1, …, 1 виділяють протокольний блок даних та сервісний блок даних (звідси випливає необхідність у ПрП і СП).

1.8.3. **Алгоритмічні рівні і рівні спецпроцесора (оброблення точок еліптичних кривих).** Алгоритми, що лежать в основі сучасних систем КЗІ, (рис. 2.3) тісно зв'язані між собою і відповідають структурі функціонального каналу. Це дозволяє прив'язати їх до рівнів еталонної моделі взаємозв'язку відкритих систем [127]. При цьому на найнижчому рівні виконується додавання елементів розширених полів Галуа (як правило – представлених багаторозрядними кодами (рис. 2.2), розрядністю до 1000 біт і більше), а на наступному - операції множення, піднесення до квадрату та інвертування елементів цих полів (представлених тими самими багаторозрядними кодами).

В еталонній моделі взаємозв'язку відкритих систем [94] кількість рівнів не оговорюється (позначається *N*). Тому для реалізації СП, кількість рівнів може бути різною, в залежності від алгоритму розв'язання поставленої задачі.

Апаратну реалізацію одного рівня (одного спецпроцесора) наведено на рис. 3.1 [12]. Відомі шифропроцесори з одним протокольним процесором і декількома спецпроцесорами, в тому числі і для опрацювання точок еліптичних кривих (рис. 3.2) [39].

Виконанню операцій на двох найнижчих рівнях і присвячена дана робота.

1.8.4. **Протокольний та виконавчий процесори в структурі спецпроцесора.** Як було показано раніше (р. 2.1), будь-який складний обчислювальний пристрій повинен складатися з двох частин – протокольної, яка реалізує функцію переходів, і виконавчої, яка реалізує функції виходів.

Протокольна частина – це, як правило, універсальний програмований процесор, виконавча – СП. Такий підхід пропонується реалізувати при проєктуванні систем захист інформації, де метою є забезпечення високого ступеня конфіденційності, продуктивності роботи, низької споживаної потужності. При цьому існують додаткові вимоги, такі як короткий строк розроблення та простота модифікації чи заміни використовуваних алгоритмів (так звана алгоритмічна

незалежність).

1.8.5. **Спецпроцесор як функціональний канал.** Представлення СП як функціонального каналу (рис. 2.1), тобто, каналу, який не передає через фізичне середовище надану йому інформацію, а обробляє її за допомогою деякого функціонального вузла і повертає назад результат оброблення, підказує можливість використання еталонної моделі взаємозв'язку відкритих систем [94] для розподілу функцій між засобами КЗІ [12].

1.8.6. **Розподіл задач між рівнями спецпроцесорів.** Розподіл задач між різними рівнями СП показано на прикладі СП, що опрацьовує ЕЦП (таблиця 1.3). Розподіл задач між рівнями дає можливість визначити СК кожного із СП.

1.9. ПЛІС, ядра та генератори ядер

**ПЛІС та їхня захищеність.** Програмована логіка (ПЛІС, ПЛМ) давно використовується для проєктування СКС. На сьогоднішній день кількість тригерів в ПЛІС сягає 5 млн., а кількість 6-входових програмовних комбінаційних схем (LUT) – 2,5 млн., що разом із сучасними, орієнтованими на використання мови С як мови описів апаратних засобів (HDL), засобами дозволяє створювати проєкти з високою апаратною складністю [106]. Надійність таких ПЛИС сягає 8 FIT (8 відмов на $10^9$ годин, приблизно 1 відмова на 14 тис. років) [203].

***Ядра для ПЛІС*** (*IP cores, IP-блоки*, *IP-ядра, VC*) - готові моделі блоків (VHDL-описи моделей функціональних вузлів) для побудови систем на кристалі (*VC* - віртуальні компоненти (*virtual components*) [206].

Розрізняють 3 основних класи ядер: 1) програмні *IP*-блоки (*soft blocks*) - блоки, специфіковані на мові опису апаратури; 2) схемотехнічні блоки (*firm blocks*) - блоки, специфіковані на рівні схемотехніки, без прив'язки до конкретної топологічної реалізації; 3) фізичні (топологічні) блоки (*hard blocks*) - блоки, специфіковані на фізичному рівні реалізації НВІС.

***Ядра для засобів*** захисту інформації**.** Відомі ядра для реалізації на ПЛІС вузлів систем захисту інформації. В основному, це вузли шифрування відповідно до алгоритмів *DES*, 3*DES*, AES, гешування відповідно до алгоритмів *SHA*-1, *SHA*-256 та *MD*-5[205], [187].

З публікацій відомі ядра для роботи з полями Галуа $GF(2^m)$ [134], [124] та ядра для виконання операцій над точками ЕК – [124], [140], [120].

Методологію проєктування генераторів ядер ПЛІС викладено в [62], особливості проєктування генераторів ядер для опрацювання елементів двійкових полів Галуа в нормальному базисі викладено в [41], [42].

***Недоліками ПЛІС*** є необхідність конфігурації після кожного ввімкнення живлення та низький захист інтелектуальної власності.

***Перехід FPGA – ASIC.*** Найбільш ефективне рішення питання конфігурації після кожного ввімкнення живлення – перехід від використання ПЛІС (*FPGA*) до використання інтегральних мікросхем спеціального призначення (*ASIC - Application-Specific Integrated Circuit*). Сучасні технології дозволяють після проєктування і відлагодження ПЛІС перейти до використання *ASIC*. Процес проєктування *ASIC* при такому підході ілюструє [190].

*Таблиця 1.3*

**Розподіл задач між рівнями (рівні представлення - відповідно до [191])**

| Рівень ШП | Рівень представлення | Тип операцій | Операції |
|---|---|---|---|
| 1 (найнижчий) | Примітиви | Операції над елементами поля Галуа у нормальній формі | Піднесення до квадрату, визначення розрядів добутку |
| 2 | Примітиви | Операції над елементами поля Галуа у нормальній та поліноміальній формах | Множення, додавання, пересилання |
| 3 | Схеми | Операції над точками еліптичних кривих, криптографічні перетворення | Додавання, подвоєння, множення на число |

***Захист інтелектуальної власності.*** Відомі ПЛІС [173], які мають вбудований незмінний багатобітний ідентифікаційний номер. Також існує можливість занесення до ПЛІС аналогічного ідентифікаційного номеру користувача. За допомогою цих номерів можна побудувати схему захисту від тиражування.

Для захисту інтелектуальної власності (ядер) від несанкціонованого використання і клонування починають використовувати ЕЦП ядер [168].

1.10. Методи генерації описів функціональних вузлів

1.10.1. **Способи опису функціональних вузлів.** Описати проєкт можна у 1) вигляді схеми; 2) на мові опису апаратних засобів (*HDL*); 3) у вигляді графа автомата.

Найбільш універсальним є *HDL*-опис. Сучасні засоби проєктування забезпечують трансляцію схем і графів у *HDL*-описи. Також існують генератори *HDL*-описів стандартних вузлів цифрової техніки – генератори ядер.

1.10.2. **Мови опису апаратних засобів.** Для опису алгоритмів та *SoC* використовують, в основному, мовні засоби. Для опису алгоритмів використовуються здебільшого мови високого рівня (*C*, *C++* та інші). Для проєктування ПЛІС та *SoC* використовують *VHDL* та *Verilog*. Для моделювання додатково пропонуються засоби, реалізовані на основи мов високого рівня (*HLL*) типу *C/C++ : SystemC, PLI/VPI/VHPI, SystemVerilog*, які разом із зручним інтерфейсом користувача забезпечують також автоматичне врахування результатів тестування на його послідовність.

Для деяких задач (опрацювання сигналів та зображень, прискорення вбудованих процесорів типу *Xilinx MicroBlaze* та *PowerPC,* цифрове опрацювання сигналів, шифрування та дешифрування відповідно до 3*DES,* наукові та фінансові обчислення) існують засоби трансляції *C*-програм в *VHDL*-описи, які розділяють процес проєктування на декілька ниток проєктування : 1) апаратного забезпечення СП, 2) його інтерфейсу з керуючим процесором та 3) програмного забезпечення керуючого процесора. Для математичних обчислень використовуються стандартні бібліотеки *math.h*.

Для переходу від промодельованих на мові *C/C++* описів розробляються вузькоспеціалізовані транслятори [61, 62]. Формується тенденція переходу від описів на рівні пересилання між регістрами (*RTL,* забезпечується засобами *HDL*) до описів на рівні електронних систем (*ESL*, забезпечується використанням мов високого рівня *HLL*) [178] з наступною автоматичною генерацією *RTL*-описів і, навіть, автоматичною генерацією переліку зв’язків для проєктування топології ПЛІС.

Крім генерації описів вузлів засоби проєктування повинні забезпечувати перевіряння вузлів вбудованого контролю, тобто мати можливість генерувати спотворені описи проєктованих вузлів. З врахуванням цього використовується вдосконалений метод проєктування описів [39, 40] функціональних вузлів (Додаток С).

Даний метод передбачає володіння розробником мовою програмування високого рівня, низького рівня та мовою описів апаратних засобів. Його розраховано на проєктування спеціалізованих вузлів. Результати його застосування (бібліотеки описів, програми-транслятори) є спеціалізованими і не можуть бути використані для розв'язання задач іншого класу.

1.11. Вузли та алгоритми засобів КЗІ

1.11.1. **Множення у поліноміальному і нормальному базисах розширених полів Галуа.** Множення у поліноміальному базисі може виконуватися : 1) методом зсуву і додавання [204], [147], [171], [177] в тому числі з використанням модифікованих комірок Гілда; 2) методом логарифмування, додавання і антилогарифмування [63]; 3) табличним методом.

Математичні основи множення у нормальному базисі [3] див. Додаток З. Помножувачі у нормальному базисі дозволяють створювати схеми з використанням динамічних елементів (що зменшує споживану потужність та розміри помножувача) [148].

1.11.2. Комірка Гілда

Відомий паралельний помножувач на основі комірок Гілда [123] (рис. 2.4, а). Для використання в помножувачах елементів розширених полів Галуа для поліноміального базису відома модифікована комірка Гілда [23] (рис. 2.4, б, в, г), яка не має вхідного та вихідного переносів, оскільки при опрацюванні елементів розширених полів Галуа відсутні переноси між розрядами їх кодів.

Саме на основі досліджень паралельного помножувача елементів розширених полів Галуа, що складається з модифікованих комірок Гілда, у даній роботі розроблено методи оцінювання складностей помножувачів.

Вузол помножувача (*Multiplier*) і вузол піднесення до квадрату - квадратор

(*Squarer*) входять до складу відомих спецпроцесорів для апаратної реалізації операцій над точками ЕК (рис. 1.1) [110].

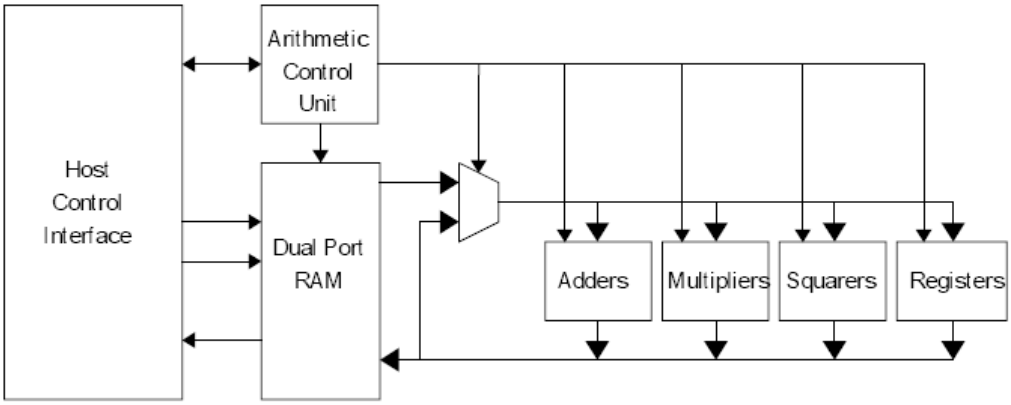



Рис. 1.1. Спецпроцесор для опрацювання точок ЕК

1.12. Перевіряння та тестування запропонованих методів та засобів

Дані про найбільш поширені математичні пакети для проведення обчислень у полях Галуа містить Додаток Ж (Таблиця Ж. 1).

Найбільше можливостей для роботи з великими полями Галуа надає пакет *Maple*, але і він забезпечує проведення обчислень тільки у поліноміальному базисі. Тому актуальною є задача розроблення засобів, які дозволяють перевіряти результати роботи в нормальному базисі.

**Функціональна надійність.** Для сучасних засобів захист інформації розрядність елементів поля може сягати тисячі біт. Апаратна реалізація помножувача таких елементів вимагає більш ніж мільйона транзисторів. Збільшення кількості транзисторів, зменшення їхніх розмірів збільшують інтенсивність відмов цифрових схем. Прогнозується, що для функціональних вузлів сучасних комп'ютерів інтенсивність відмов збільшиться до величини 1/100. Для запобіганню цього розробляються нові методи виявлення та виправлення помилок.

У роботах останніх років звертається увага на вбудовані апаратні методи виявлення помилок [14]. Також використовуються програмні методи повторного виконання операцій з переставленими місцями операндами.

1.13. Маскування роботи засобів КЗІ

1.13.1. **Методи атак на засоби криптографічного захисту інформації.** Засоби КЗІ повинні мати захист від атак (Додаток Г) [134]. Для атак використовуються

різні методи [176], [134]: 1) охолодження пристроїв до наднизьких температур, 2) хімічне розчинення корпусів мікросхем, 3) досліджування топології кристалів за допомогою електронних мікроскопів, 4) під'єднання до кристалів за допомогою надзвичайно тонких голок та інші методи.

Споживана потужність цифрових схем є високоінформативним джерелом інформації про стан цих схем. Її використовують і при тестуванні і дослідженнях роботи цифрових схем [138], і для злому засобів КЗІ (side-channel attacks – атаки сторонніми каналами [88]).

І атаки на основі споживаної потужності, і атаки на основі електромагнітного випромінювання ґрунтуються на різному споживанні КМОН-транзисторних схем в залежності від частоти їхнього переключення. Якщо при деяких алгоритмах кількість операцій при нульовому значенні деякого розряду операнда менша від кількості операцій при його одиничному значенні, це може дозволити визначити шляхом виміру споживаної потужності або електромагнітного випромінювання значення усіх розрядів операнда [166].

1.13.2. **Метод захисту від атак – маскування.** Одним з методів захисту від атак є маскування.

Для маскування роботи операційних вузлів в основному використовують [125]: 1) вирівнювання тривалості виконання операцій в залежності від значення окремих розрядів операндів (Рис. Г.3, Рис. Г.4 [125]); 2) робота вузлів без пауз; 3) паралельна робота додаткових аналогічних вузлів, які виконують операції над випадковими або псевдовипадковими числами; 4) робота вузлів без пауз тільки під час виконання необхідних алгоритмів – для зменшення споживаної потужності. У роботі буде розвинуто метод маскування роботи вузлів знаходження обернених елементів двійкових полів Галуа, коди яких представлено у поліноміальному базисі.

1.14. Висновки до розділу 1

У **першому** розділі проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП). Підкреслено, що із поширенням КФС частка їхнього

обладнання, яке використовує КЗІ, стає все меншою, що стає неприпустимим у зв'язку із постійним збільшенням кількості атак на КС, а останнім часом і на КФС. Підкреслено, що навіть захищені системи стають вразливими з появою квантових комп'ютерів. Серед задач КЗІ є задача розроблення, використання і вдосконалення засобів опрацювання цифрових підписів, яке передбачає використання операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

Для визначення найкращого варіанту реалізації окремих засобів КЗІ необхідно аналізувати складності алгоритмів їх роботи, для чого найкраще підходить *SH*-модель алгоритму. При апаратній реалізації алгоритмів захищеність інформації забезпечується спеціальною апаратурою – спеціалізованими операційними вузлами, які разом утворюють спецпроцесор (СП, для засобів КЗІ – шифропроцесор (ШП) або криптопроцесор (КП)). Найважливішими перевагами апаратної реалізації засобів КЗІ є: 1) кращі швидкісні характеристики; 2) більша фізична захищеність від побічних електромагнітних випромінювань і від безпосереднього фізичного впливу на пристрій, у якому здійснюється захист інформації та збереження ключової інформації; 3) зменшення споживаної потужності.

У розділі зроблено огляд стандартів опрацювання ЕЦП, які діють в Україні та світі. Принципи використання електронного цифрового підпису розглянуто також.

Математичною основою опрацювання ЕЦП є еліптичні криві (на основі використання яких можна організувати і постквантову криптографію) та розширені поля Галуа, які також розглянуто в першому розділі. Особливу увагу приділено представленню елементів розширених полів Галуа у ШП та виконанню основних операцій над елементами полів та оцінюванню апаратної та структурної складності вузлів для виконання цих операцій.

У розділі проаналізовано модель взаємозв'язку відкритих систем, на основі якої можуть бути реалізовані багаторівневі системи захисту інформації, розглянуто методи проєктування багаторівневих систем. Також проаналізовано елементну базу для реалізації сучасних комп'ютерних систем та їх складових – ПЛІС та методи проєктування та тестування елементів КЗІ на їх основі.

Як один із засобів протистояння атакам на засоби КЗІ розглянуто маскування

їх роботи.

При цьому: визначено актуальність, доцільність та необхідність розроблення засобів КЗІ; КФС визначено як перспективну галузь застосування засобів КЗІ; визначено необхідність розроблення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК; визначено необхідність детального аналізу математичних основ та абстрактних алгоритмів опрацювання елементів розширених полів Галуа для розроблення на їх основі структурних алгоритмів.

У даному розділі показано сучасні підходи до побудови засобів КЗІ – виконання операцій і методи контролю результатів обчислень у полях Галуа. Виділено найбільш працемісткі операції (множення та знаходження обернених елементів), які вимагають апаратної реалізації. Проаналізовано ресурси для перевіряння результатів виконання окремих операцій над елементами полів Галуа.

Проведений аналіз визначив першочергове завдання роботи - наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

# РОЗДІЛ 2
# УЗАГАЛЬНЕНІ ВИМОГИ ТА АРХІТЕКТУРНІ ПРИНЦИПИ ПОБУДОВИ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

## 2.1. Вибір і обґрунтування напряму досліджень

У першому розділі показано, що здійснювати КЗІ можна і програмними, і апаратними (на основі операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК) засобами.

У першому розділі визначена невідповідність українських стандартів міжнародним. Міжнародні стандарти передбачають використання двійкових полів Галуа набагато більшого степеня. Перспектива появи квантових комп'ютерів вимагає використання розширених полів Галуа з порядком, який також перевищує вимоги сучасних стандартів. Другий розділ присвячений визначенню шляхів розв'язання цієї основної задачі - створення методів та засобів опрацювання елементів полів Галуа, які забезпечують дотримання і міжнародних, і українських стандартів, і можуть протистояти використанню методів злому КЗІ, що будуються на використанні квантових комп'ютерів.

Цим досягається розв'язання у роботі важливої науково-прикладної задачі: визначення підходів та методів і наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

За результатами аналізу формується уява про багаторівневу структуру операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. Верхній рівень забезпечує обмін інформацією із зовнішнім середовищем. Нижній (власне спеціалізований, СП) – забезпечує виконання специфічних для даного завдання операцій. Розвитком цієї ідеї є погляд на СП як на також багаторівневу відкриту систему.

За основу для проведення досліджень взято модель взаємозв'язку відкритих

систем. За цією моделлю спеціалізовані комп'ютерні засоби, спецпроцесори, представлено як функціональні канали, які мають багаторівневу багатозадачну структуру (рис. 2.1).

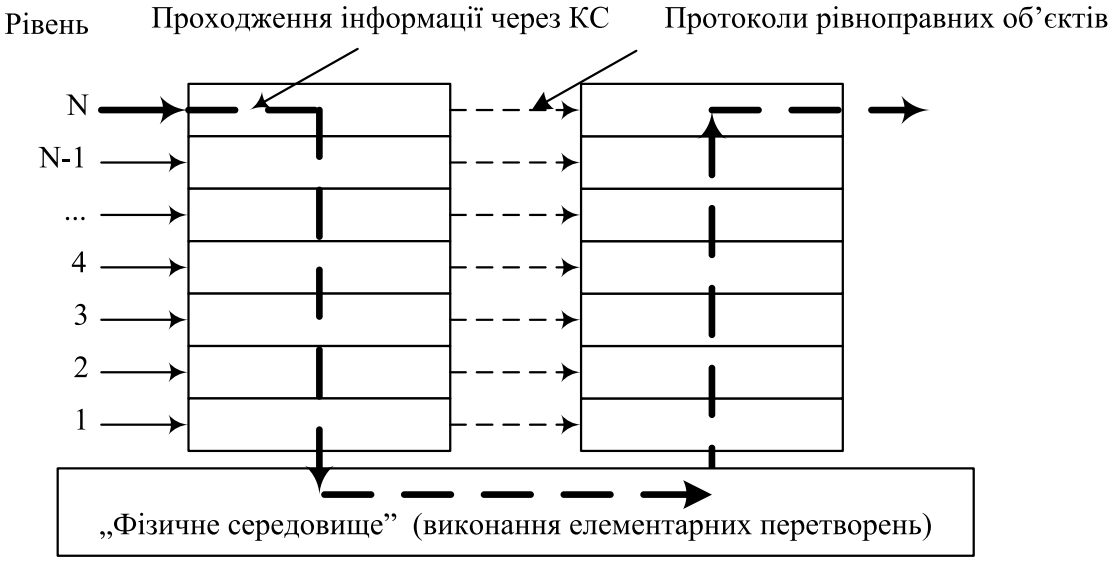



Рис. 2.1. Функціональний канал

2.2. Основи проєктування засобів КЗІ на базі операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

На сучасному етапі, коли КЗІ впроваджуються у КФС, важливим стає забезпечення їх роботи у реальному масштабі часу. Це вимагає використання швидкодіючих апаратних рішень – спецпроцесорів, які реалізуються в програмовних логічних інтегральних схемах (ПЛІС). Як базу для проєктування засобів КЗІ взято багаторівневий спецпроцесора (СП), який при опрацюванні цифрових підписів виконує операції над точками еліптичних кривих. Проектування такого спецпроцесора вимагає використання спеціальних розділів математики: полів Галуа, еліптичних кривих (ЕК) тощо. Елементи полів Галуа та точки ЕК представляються за допомогою багаторозрядних двійкових кодів (розрядністю сотні і тисячі біт, рис. 2.2).

СП вимагає оригінальних засобів для виконання операцій над ними. СП функціонує на основі таких теоретичних положеннях, які дозволяють розглядати його як спеціалізовану комп'ютерну систему (СКС) з архітектурою, відмінною від відомих архітектур КЗ.

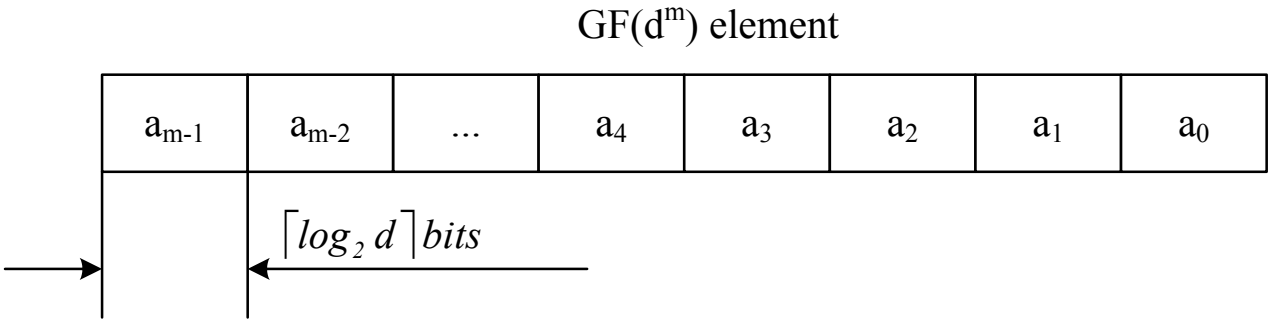



Рис. 2.2. Представлення елементів розширених полів Галуа

2.2.1. Особливості реалізації засобів КЗІ на ПЛІС

Одним з основних елементів для проєктування функціональних вузлів спеціалізованих комп'ютерів є ПЛІС, у яких останнім часом з'явилися такі важливі властивості:

1) ПЛІС полегшує наступний швидкий перехід до *ASIC*, тобто, до масового виробництва, апаратної реалізації алгоритмів та збереження всередині мікросхеми проміжних результатів при виконанні цих алгоритмів (р. 1.9);

2) сучасні ПЛІС забезпечують збереження інтелектуальної власності та ускладнюють несанкціоноване тиражування та «зворотне проєктування» (*Reverse engineering*, р. 1.9).

Від сучасних комп'ютерних засобів вимагається дотримування принципів побудови відкритих систем, що орієнтує на використання відкритих стандартів.

В Україні діють декілька стандартів на ЕЦП: міждержавний стандарт ГОСТ 34.310-95 та орієнтований на використання еліптичних кривих національний стандарт України ДСТУ 4145-2002. Підтримку застосуванню ЕЦП надають стандарти, що забезпечують неспростовність ЕЦП, розкривають механізми роботи ЕЦП на основі ідентифікаторів та сертифікатів. Також стандартизовано методи роботи із еліптичними кривими ДСТУ ISO/IEC 15946-1: 2015, установлення ключів ДСТУ ISO/IEC 15946-3: 2008, оновлено процедури шифрування ДСТУ 7624:2014 і гешування ДСТУ 7564:2014.

Вирішення завдань захисту від несанкціонованого використання і від пошкодження інформації відомі і широко використовується на практиці. Але сучасні методи, які базуються на використанні розширених полів Галуа $GF(p^m)$, де $p > 2$, та суперсингулярних еліптичних кривих і які здатні протистояти

використанню квантових комп'ютерів з метою злому системи захисту, на сьогоднішній день розроблено недостатньо, особливо це стосується апаратних методів.

Першим кроком розв'язання поставленої задачі є вибір поля Галуа $GF(p^m)$, яке забезпечить створення операційних вузлів з найкращими характеристиками в порівняння з іншими полями. Для цього необхідно порівнювати вузли, створені для різних полів – порівнювати їхні складності. Щоб не порівнювати кожний вузол з аналогічними вузлами інших полів, пропонується за базу для порівняння взяти вузли для полів, які на сьогоднішній день найширше використовуються – для двійкових розширених полів $GF(2^M)$. При цьому обов'язково повинна дотримуватися умова – усі розширені поля Галуа повинні бути з приблизно однаковою кількістю елементів (з приблизно однаковим порядком), тобто, $p^m \approx 2^M$.

Вищесказане визначає актуальність створення методів і засобів проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. І в роботі пропонуються рішення цього завдання (Таблиця 2.1).

## 2.3. Основні архітектурні принципи побудови операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

За результатами проведеного аналізу (Розділ 1) формується уява про організацію операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК як про багаторівневу СКС. Для забезпечення функціональної гнучкості спеціалізовані операційні пристрої будується за багаторівневою схемою у відповідності до відкритої моделі взаємозв'язку відкритих систем і складаються з:

протокольної частини, ядром якої є універсальний процесор (у цій роботі не розглядаються);

спеціалізованої частини (власне операційний пристрій, часто - на базі ПЛІС) з реалізованими в ній додатковими операційними вузлами, які використовуються для розв'язання задач, що не можуть бути вирішені за потрібний час програмно універсальним процесором;

для прискореного опрацювання багаторозрядних елементів полів Галуа та точок еліптичних кривих здійснюється паралельне опрацювання визначеної

кількості їхніх окремих біт. Частина операційного пристрою, яка опрацьовує таку виділену кількість біт називається секцією. До складу пристрою входить декілька секцій (однакових чи різних), операційні пристрої в цьому випадку називаються секційними;

якщо секція опрацьовує відразу усі біти кодів, то такий пристрій називається паралельним;

кількість біт може змінюватися під час проєктування без змін, не пов’язаних із ними параметрів, операційні пристрої в цьому випадку називаються конфігурованими.

*Таблиця 2.1*

**Основні вимоги до архітектури та методів створення КЗ забезпечення КЗІ**

| Вимоги | Аналіз, розділ | Чим забезпечується рішення задачі | Реалізація, розділ |
|---|---|---|---|
| Апаратна реалізація алгоритмів | 1.2.8, 1.9 | використанням сучасних технологічних рішень – ПЛІС, ядер | 2.2.1 |
| надійність | 1.9 | використанням сучасних технологічних рішень – ПЛІС, ядер | 2.2.1 |
| функціональна надійність | 1.12 | системним, функціональним та логічним моделюванням, захистом інтелектуальної власності, реалізованої у вигляді ядер ПЛІС, застосуванням вбудованого тестування | 2.14 |
| повинна бути реалізована багаторівнева програмно-апаратна структура | 1.8 | проєктуванням багаторівневих ієрархічних структур з обґрунтованим розподілом ресурсів між рівнями | 3.1 |
| можливість проведення модернізації та модифікацій | 1.9 | використанням сучасних технологічних рішень – ПЛІС, ядер, моделюванням на мовах високого рівня з автоматичним переходом на мови описів апаратного забезпечення | 2.2.1 |
| маскування роботи засобів КЗІ | 1.13 | вирівнювання часу роботи засобів КЗІ | 2.14, 3.4, 3.5 |
| відкритість | 1.4.1, | відповідність вимогам відкритих стандартів | 3.1 |
| використання сучасної на момент проєктування елементної бази | 1.9 | використанням сучасних технологічних рішень – ПЛІС, ядер | 2.2.1 |

Разом ПрП і СП у ПЛІС утворюють багаторівневу КС. При цьому ПрП виконує функції верхніх рівнів, а СП – нижніх, якщо ставити їм у відповідність рівні еталонної моделі взаємозв’язку відкритих систем [94].

2.4. Узагальнена модель операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

В основу проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК пропонується, як узагальнену модель, покласти еталонну модель взаємозв'язку відкритих систем, також пропонуються засоби реалізації цієї моделі (Таблиця 2.2).

Уточнення узагальненої моделі для операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК полягає в розміщенні останніх на нижніх рівнях еталонної моделі взаємозв'язку відкритих систем (рис. 2.3). Розробленню уточнених моделей та структурних алгоритмів їх роботи присвячено наступні підрозділи цієї роботи.

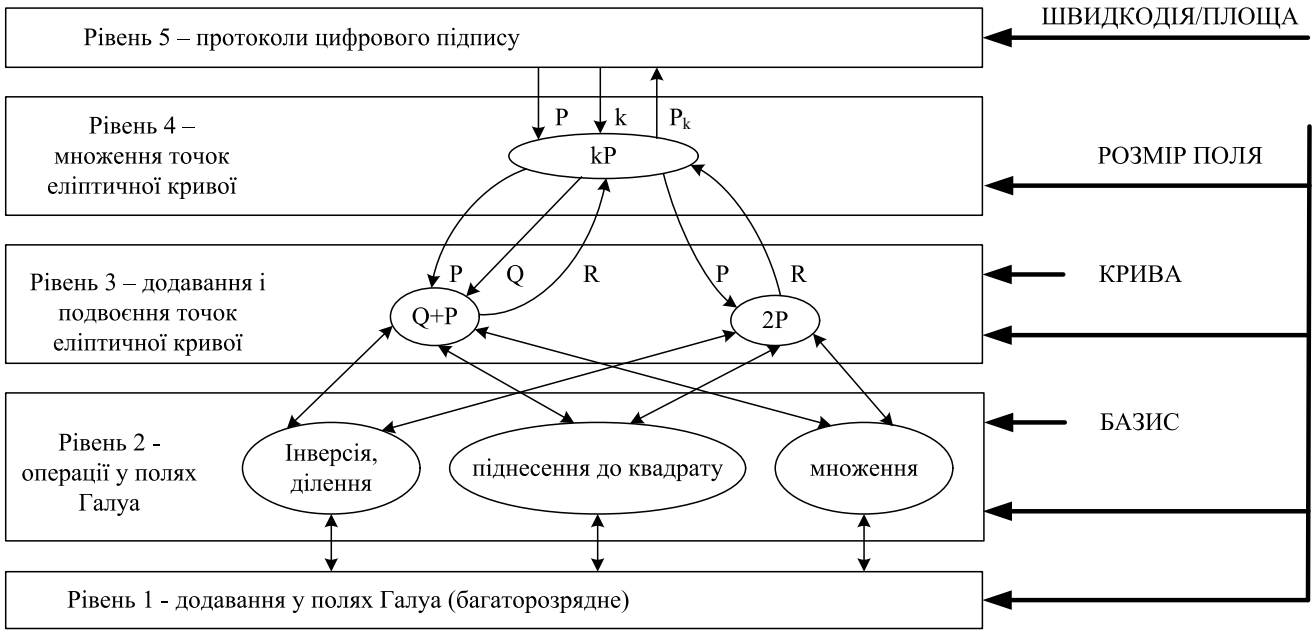



Рис. 2.3. Рівні алгоритмів КЗІ на основі еліптичних кривих

Основними операціями у розширених полях Галуа $GF(p^m)$, виконання яких вимагає найбільшого часу, є обчислення оберненого елемента та множення. Операції над елементами розширених полів Галуа $GF(p^m)$ використовуються для виконання операцій над точками ЕК (додавання точок, подвоєння, множення на константу). У дисертаційній роботі розробляються структурні алгоритми виконання операцій над елементами поля Галуа $GF(p^m)$ з великими значеннями $m$ [93], проводиться реалізація розроблених структурних алгоритмів у вигляді операційних пристроїв, які здійснюють перетворення за стандартами [93], [98].

*Таблиця 2.2*

**Забезпечення адаптації структурованої моделі**

| Що необхідно розробити для рішення задачі | Аналіз, розділ | Реалізація, розділ |
|---|---|---|
| модель пристрою для опрацювання елементів полів Галуа *GF(dm)* (у поліноміальному базисі) | 0, 1.8 | Розділ 3 |

2.5. Підходи до проєктування уточнених моделей операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

З наведеного аналізу (Розділ 1) випливає, що розв’язати важливу і актуальну науково-прикладну задачу створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК можливо тільки на стику багатьох наукових напрямів.

При їх проєктуванні необхідно враховувати висновки теорії обчислювальних машин, теорії обчислювальних систем, теорії проєктування СКС (р. 1.8), використовувати модель взаємозв’язку відкритих систем (р. 1.8).

Для реалізації елементів спецпроцесорів на ПЛІС потрібно використовувати теорію проєктування НВІС (р. 1.9), для створення пристроїв керування необхідно використовувати теорію графів, теорію алгоритмів, теорію цифрових автоматів (р. 1.2). Для розроблення методів опрацювання елементів полів Галуа потрібно враховувати положення і висновки теорії чисел, теорії залишків, теорії обчислень, теорії груп, теорії матриць, теорії інформації (р. 0), для проєктування СП потрібні результати теорії кодування, для створення моделі СП та для дослідження його роботи необхідно задіяти теорію моделей, теорію програмування, обчислювальну математику, моделювання алгоритмів та апаратних засобів комп’ютерів (р. 1.10).

Перевіряння отриманих результатів повинне здійснюватися відповідно до теорії випробовувань шляхом моделювання.

Для розроблення та вдосконалення методів оцінювання складності, для маскування та вбудованого контролю операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК необхідно попередньо розв’язати такі важливі і актуальні задачі:

розроблення моделі операційних вузлів для полів Галуа, які використовуються

при КЗІ на основі ЕК у відповідності до сучасних стандартів;

розроблення структурних алгоритмів роботи операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

забезпечення зв'язку процесів моделюванням алгоритмів роботи вузлів спецпроцесорів, створення описів функціональних вузлів, моделювання роботи функціональних вузлів;

вибір сучасної елементної бази, технологій та засобів проєктування;

розроблення засобу генерації описів функціональних вузлів операційних пристроїв.

2.6. Деталізація вимог щодо захисту роботи засобів КЗІ

Для забезпечення захисту роботи операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК повинні задовольнятися наведені нижче вимоги (таблиця 2.3).

*Таблиця 2.3*

**Забезпечення конфіденційної складової**

| Вимоги | Аналіз, розділ | Реалізація, розділ |
|---|---|---|
| апаратна реалізація алгоритмів | 1.2.8 | Розділ 3 |
| проєктування спеціалізованих мікросхем (на основі ПЛІС) | 1.9 | Розділ 3 |
| маскування роботи вузлів, що реалізують обрані алгоритми | 1.13 | Розділ 3 |

2.7. Деталізація вимоги щодо роботи із електронним цифровим підписом

Для використання при роботі з ЕЦП операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК останні повинні задовольняти вимогам (Таблиця 2.4).

2.8. Загальна методика проведення дисертаційних досліджень

У відповідності до виявлених напрямків досліджень робота складається з досліджень принципів побудови операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК як багаторівневих структур (р. 1.8.3), дослідження принципів реалізації основних операцій, характерних для операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК: множення

елементів полів Галуа і знаходження обернених елементів, синтез на основі проведених досліджень операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК (Розділ 3), дослідження спроєктованих операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК та представлення результатів їх впровадження (Розділ 4).

*Таблиця 2.4*

**Вимоги щодо роботи із ЕЦП**

| Вимоги | Аналіз, розділ | Реалізація, розділ |
|---|---|---|
| Опрацювання полів Галуа, визначеними міжнародними і національними стандартами України | 1.4.1 | Розділ 3 |
| Опрацювання ЕК, визначеними міжнародними і національними стандартами України | 1.4.1 | Розділ 3 |
| Опрацювання полів Галуа, які забезпечують меншу апаратну, часову, ємнісну та структурну складність обчислень при однакових інших характеристиках | 1.7, 1.11 | Розділ 3 |
| Використання поліноміального базису | 1.7, 1.11 | Розділ 3 |
| Проєктування багаторівневих СП | 1.8 | Розділ 3 |

2.9. Метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$

Метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ пропонується як метод знаходження розширеного поля Галуа, у якому обрані характеристики СП будуть найкращими, що забезпечить створення СП для «найкращого» поля (далі цей термін буде вживатися без лапок). Підхід базується на оцінювання складностей одного з найважливіших вузлів СП - помножувача (Таблиця 2.5). Для аналізу обрано паралельний помножувач на основі модифікованих комірок Гілда (рис. 2.4).

2.9.1. Основи методу

Запропонований метод оцінювання вузлів, що опрацьовують елементи розширених полів Галуа, має суттєву умову використання – розширені поля Галуа повинні бути з приблизно однаковою кількістю елементів (з приблизно однаковим порядком $p^m$).

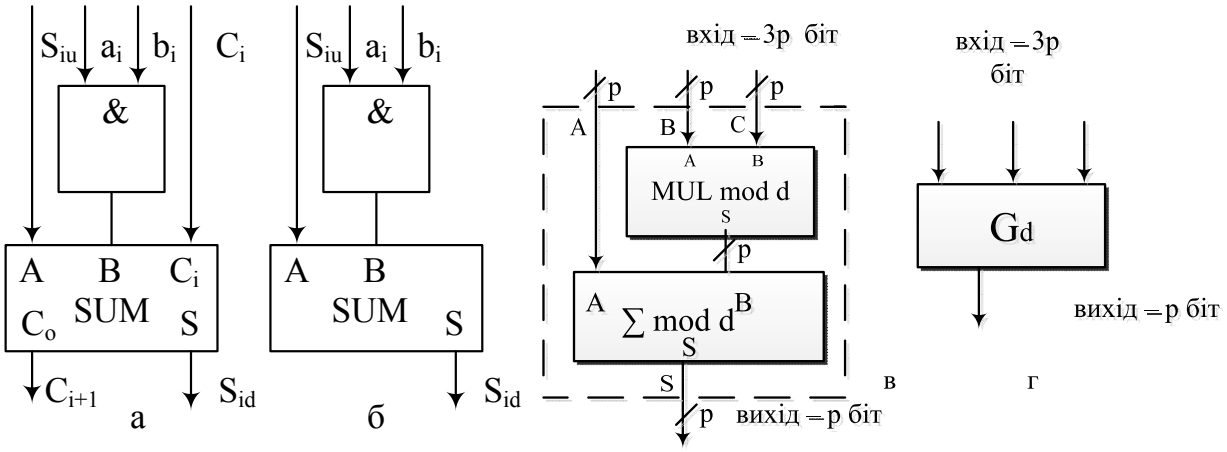



Рис. 2.4. Класична (а) та модифікована комірки Гілда (б, в) для поля Галуа GF($d^m$). Графічний символ модифікованої комірки Гілда (г).

Порядок застосування методу:

обирається розширене поле Галуа;

обирається базис представлення елементів полів Галуа (обрано - поліноміальний базис);

обираються базові елементи помножувача (обрано модифіковану комірку Гілда);

обирається структура базових елементів;

обирається структура помножувача (обрано помножувач з матричною структурою на основі модифікованих комірок Гілда;

*Таблиця 2.5*

**Визначення найкращого поля для створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК**

| Що необхідно розробити для рішення задачі | Аналіз, розділ | Реалізація, розділ |
|---|---|---|
| Оцінювання часової складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ | 1.2.7, 1.7 | 2.10 |
| Оцінювання структурної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ у нормальному та поліноміальному базисах | 1.2.7, 1.7 | 2.11 |
| Оцінювання ємнісної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ | 1.2.7, 1.7 | 2.12 |
| Метод оцінювання складності злому апаратних засобів КЗІ | 1.2.7, 1.7 | 2.13 |

проводиться аналіз обраного типу складності, відносні значення параметрів

складності формуються по відношенню до аналогічних параметрів розширеного двійкового поля;

дослідження повторюються для всіх обраних для аналізу розширених полів Галуа;

фіксуються результати дослідження;

визначається найкраще поле.

Метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ у цій роботі, в основному, базується на представленні помножувача для поліноміального базису як паралельного помножувача у вигляді набору модифікованих комірок Гілда.

Інші типи помножувачів можна отримати трансформацією паралельного помножувача, вони залишаються за рамками цієї роботи.

Методи оцінювання апаратної складності добре розроблені і реалізовані в засобах проєктування ПЛІС. Тому в даній роботі основна увага приділена розробленню методів оцінювання часової, структурної та ємнісної складності помножувачів елементів розширених полів Галуа.

2.9.2. Матричний помножувач для поліноміального базису на основі модифікованих комірок Гілда для розширених полів Галуа

На рис. 2.5 схематично показано функціональну схему помножувача двох елементів поля $GF(d^m)$ з використанням модифікованих комірок Гілда, детальна схема яких наведена на рис. 2.4, в. На рисунках позначено: $q_i$ – розряди утворюючого поле полінома, $p = \lceil log_2 d \rceil$ – кількість біт у записі числа d. Схема рис. 2.5 містить додаткові вузли f, які визначають на який коефіцієнт необхідно помножувати утворюючий поліном при зведенні результату добутку. Ці елементи впливають на часову складність помножувача, але можна показати [21], що незначна модифікація схеми рис. 2.5 дозволяє вилучити з неї вузли f (рис. 2.6). Для цього достатньо на відмічені позначкою інверсії входи комірок Гілда Gn подавати інверсні в обраному полі значення відповідних кодів (при цьому на позначених інверсією виходах елементів будуть формуватися інверсні в обраному полі коди). Формули, які доводять можливість такої заміни наведено на рис. 2.6. У зв’язку з

рівнозначністю схем рис. 2.5 і рис. 2.6 далі при аналізі буде виконуватися посилання на рис. 2.5.

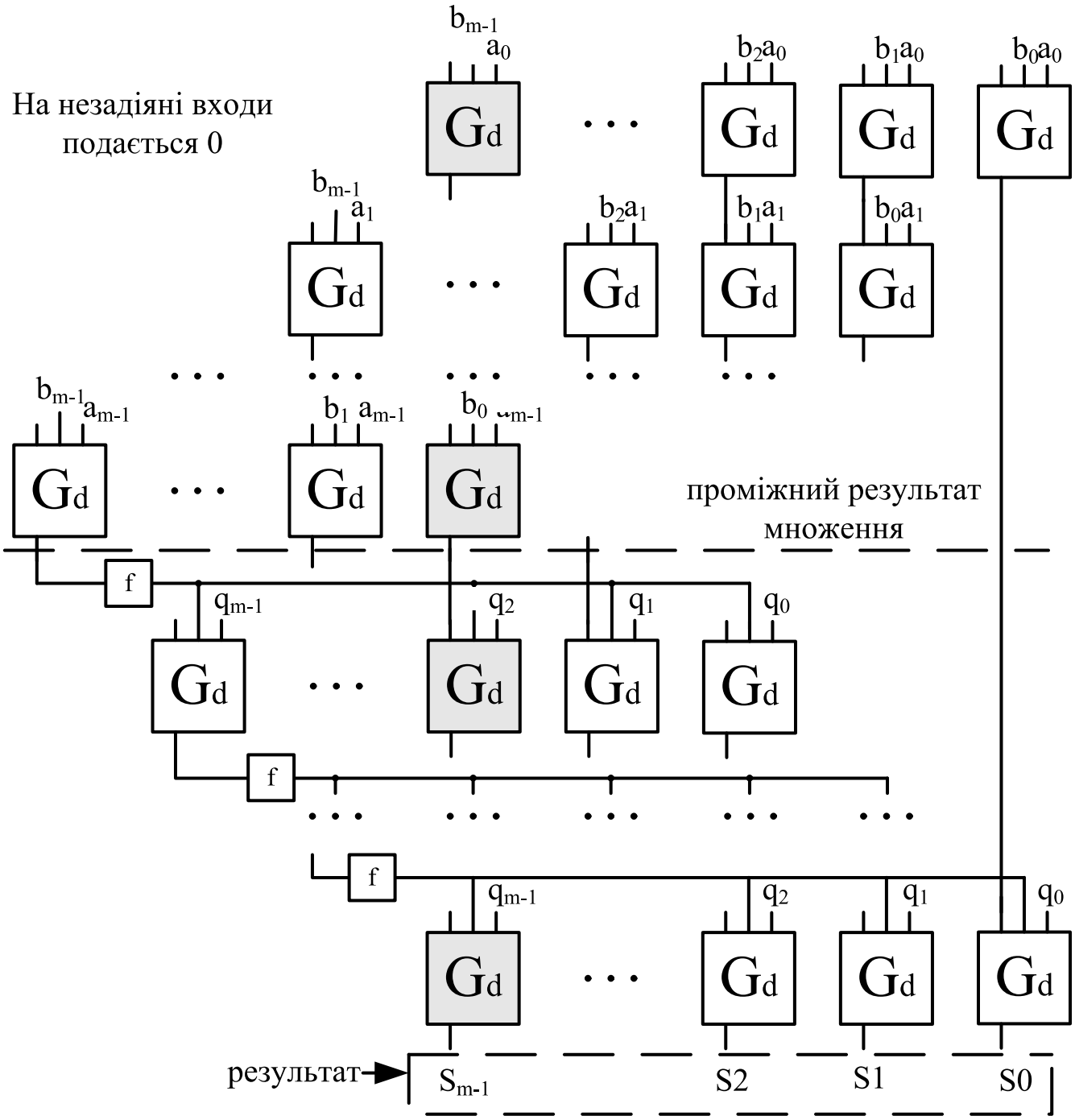



Рис. 2.5. Помножувач для поля GF($d^m$) з використанням модифікованих комірок Гілда

2.10. Оцінювання часової складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$

Одним з можливих варіантів розв'язку задачі зменшення складності операційних пристроїв є перехід на використання полів Галуа з характеристикою *n*,

більшою ніж 2, в першу чергу – з характеристикою 3 [49]. При зміні поля можуть змінитися часові характеристики помножувача.

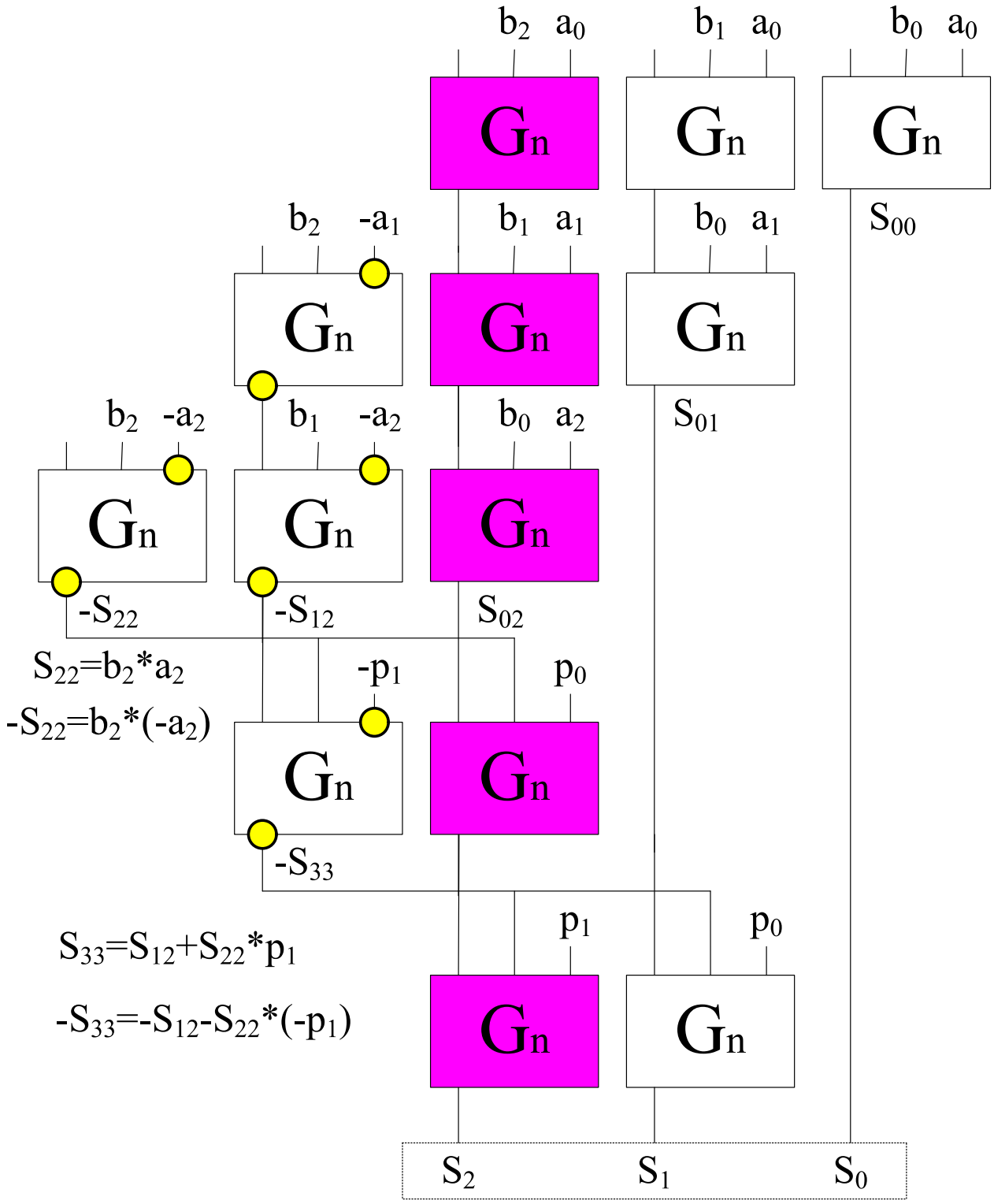



Рис. 2.6. Помножувач без вузла f (усі операції виконуються за модулем d=3)

Запропонований метод [70], [44], [155] передбачає оцінювання помножувачів для розширених полів Галуа GF($d^m$) з характеристиками $d \geq 2$, і з приблизно

однаковою кількістю елементів $d^m \approx 2^n$ ($m \approx log_d 2^n = \frac{n}{log_2 d}$) для визначення поля, в якому помножувач буде мати найменшу часову складність.

В ході аналізу визначається відносна щодо двійкового розширеного поля Галуа $GF(2^n)$ часова складність як найбільша відносна затримка проходження сигналів через помножувач (найбільша затримка виникає під час формування розряду $S_{m-1}$. Вона складається із затримок послідовно з'єднаних комірок Гілда, що утворюють вертикальний стовпчик, на виході якого формується розряд $S_{m-1}$. Ця найбільша затримка $t_{Mul} = 2mt_G$, де $t_G$ – затримка сигналів однією коміркою Гілда (рис. 2.4)). Затримка сигналів базовим елементом визначається як кількість послідовно з'єднаних комбінаційних логічних програмованих вузлів LUT, що входять до складу ПЛІС [*201*], [*202*];

2.10.1. Формальний підхід до визначення часової складності модифікованої комірки Гілда

При формальному підході комірка Гілда розглядається як «чорна скринька» з відомою кількістю входів та виходів і з невідомою внутрішньою структурою. Це відповідає табличному методу обчислення (у даному випадку – множення) і реалізації помножувача у вигляді ПЗП на основі LUT.

Модифіковані комірки Гілда при реалізації на ПЛІС будуються з програмованих комбінаційних логічних вузлів (LUTv), кожний з яких має v входів та 1 вихід і може бути запрограмований на реалізацію довільної логічної функції v змінних. До складу сучасних ПЛІС входять логічні комбінаційні вузли LUTv з кількістю входів v=4 та v=6 (ПЛІС Spartan 3 та Spartan 6, відповідно, [*201*], [*202*]). При необхідності утворення з таких LUTv j-входової комбінаційної схеми LUTj з і виходами необхідно задіяти $N_{j,i} = i(2^{j-v+1}-1)$ LUTv ($j > v$, $i > 0$, рис. 2.7). При цьому послідовно буде з'єднано $M_{j,i} = (j-v+1)$ LUTv. Якщо $j \le v$, то $N_{j,i} = i$, $M_{j,i} = 1$.

Модифікована комірка Гілда має 3p входів ($p = \lceil log_2 d \rceil$ – кількість біт у записі числа d). Для випадку ($3p > v$, $v = 4$) $p>1$, що відповідає полям $GF(d^m)$ з характеристикою $d > 2$, затримка модифікованої комірки Гілда дорівнює $t_G = (3p-v+1)t_v = (3p-3)t_v$, де $t_v$ – затримка одного елемента LUTv, тоді

$t_{Mul}=2mt_G=(3p-v+1)t_v = 2m\,(3p-3)t_v = C_{t,d}t_v$, де $C_{t,d} = 2m(3p-v+1) = 2m(3p-3)$ - часова складність помножувача для розширеного поля Галуа GF($d^m$).

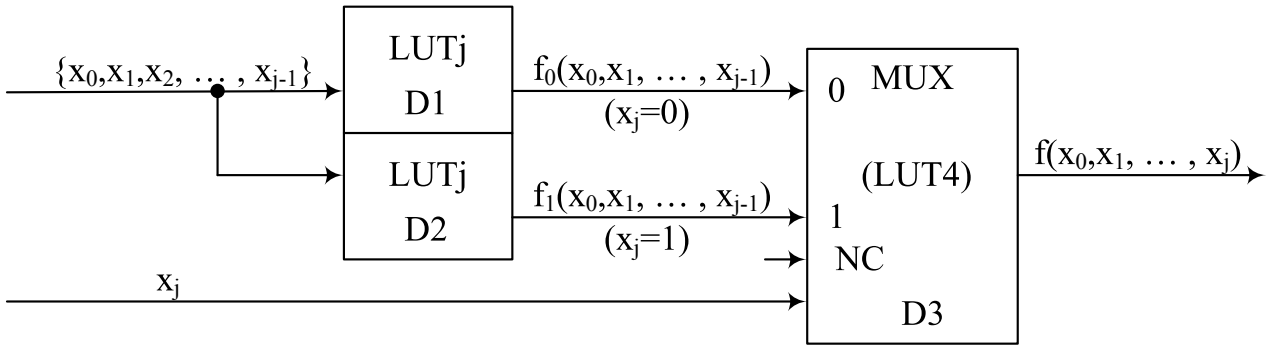



Рис. 2.7. Утворення LUTj з LUT(j-1)

Для випадку ($3p \le v$, $v = 4$) $p = 1$, що відповідає двійковим полям GF($2^n$) з характеристикою $d = 2$, затримка модифікованої комірки Гілда дорівнює $t_G=t_v$, тоді $t_{Mul}=2nt_G=2nt_v=C_{t,2}t_v$, де $C_{t,2} = 2n$ - часова складність помножувача для двійкового поля Галуа GF($2^n$).

2.10.2. Вибір поля Галуа на основі оцінювання часової складності помножувачів

При зміні поля можуть змінитися часові характеристики помножувача. У [44], [70] з цієї точки зору оцінюється помножувачі для розширених полів Галуа *GF($d^n$)* з характеристиками *d*, більшими за 2, і з приблизно однаковою кількістю елементів $d^n \approx 2^m$, що реалізуються на ПЛІС. Для аналізу обрано поліноміальний базис представлення елементів полів Галуа та помножувач з матричною структурою на основі модифікованих комірок Гілда. Показано, що часова складність помножувача для поля GF($3^n$) для ПЛІС з 6-входовими комбінаційними програмованими логічними вузлами приблизно в 1,5 разів менша за часову складність помножувача для поля Галуа GF($2^m$).

За базу для оцінювання часової складності та для визначення кількості елементів поля [70] береться розширене двійкове поле Галуа GF($2^m$), тоді $d^m \approx 2^n$, $m \approx log_d\, 2^n = \dfrac{n}{log_2\, d}$, часова складність для розширеного поля з характеристикою d

$C_{t,d} = \frac{2n(3\lceil log_2 d \rceil - v + 1)}{log_2 d}$. Відносно часової складності розширеного двійкового поля Галуа GF($2^m$) часова складності розширеного поля Галуа GF($d^n$) (відносна часова складність $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$.

$R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 3)}$ для v=4, $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 5)}$ для v=6. Якщо $R_{d,2} > 1$, то розширене поле з характеристикою d має меншу часову складність в порівнянні із розширеним двійковим полем. Як видно, перевагу перед двійковим полем має тільки поле з характеристикою d=3 (серед простих характеристик) при використанні LUT6 з 6 входами (рис. 2.8).

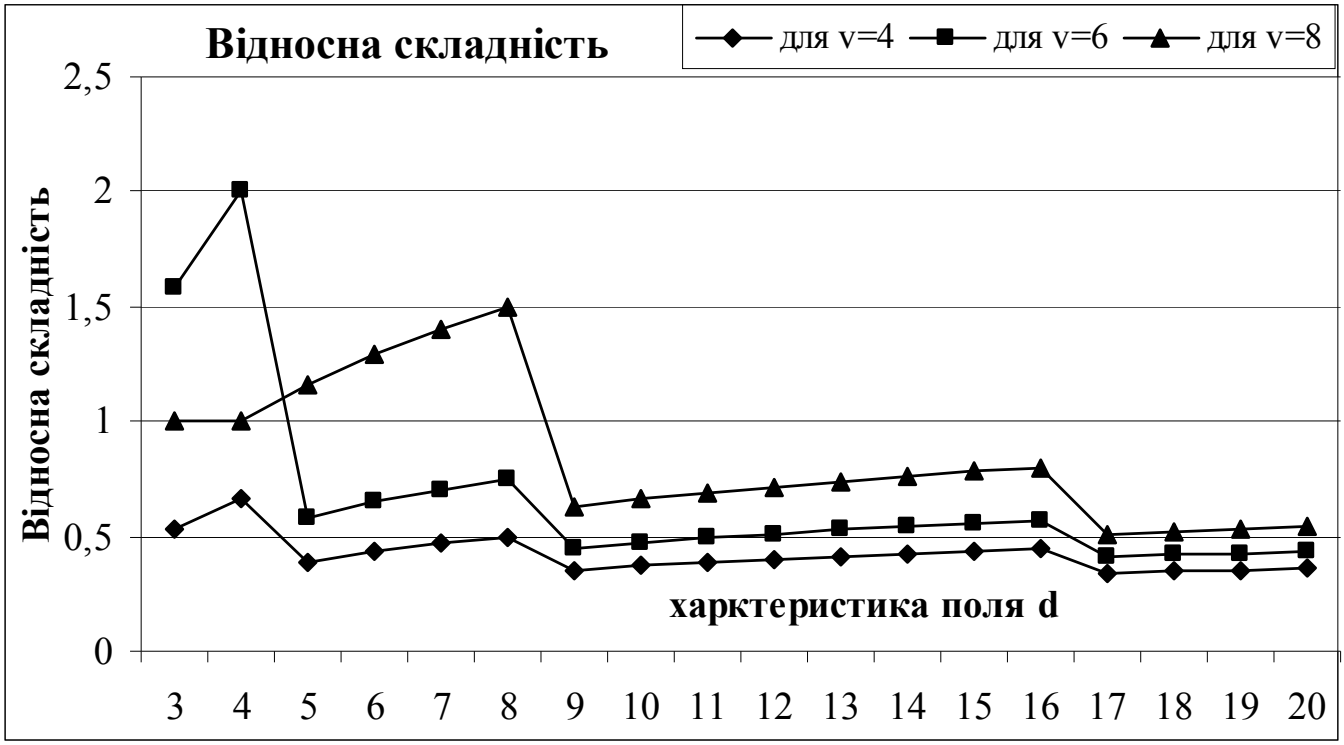



Рис. 2.8. Відносні часові складності («чорна скринька»)

На рис. 2.8 також показано оцінку часової складності при реалізації помножувача на гіпотетичній ПЛІС з логічними комірками, які мають 8 входів (LUT8). В цьому випадку перевагу перед двійковими полями будуть додатково мати розширені поля з простими характеристиками d = 5 та d = 7.

Найкращим полем є поле GF($3^m$) для ПЛІС з 6-входовими комбінаційними програмованими логічними вузлами (LUT6), часова складність помножувача для

нього приблизно в 1,5 разів менша за часову складність помножувача для поля Галуа GF($2^m$).

Запропонований метод може бути застосовано при аналізі інших помножувачів, а також при аналізі помножувачів для полів з нормальним базисом представлення елементів поля.

2.10.3. Визначення часової складності модифікованої комірки Гілда з врахуванням її внутрішньої структури (помножувача і суматора за модулем d)

При цьому підході [21] комірка Гілда розглядається як така, що складається з модульного помножувача та модульного суматора (рис. 2.4), кожний з цих елементів має 2p входів та p виходів.

Для випадку ($3p > v$, $v = 4$) $p>1$, що відповідає полям з характеристикою $d > 2$, затримка модифікованої комірки Гілда дорівнює $t_G = 2(2p-v+1)t_v = 2(2p-3)t_v$, де $t_v$ – затримка одного елемента LUTv, а $t_{Mul}=(2m-1)t_G=2(2m-1)(2p-v+1)t_v = 2(2m-1)(2p-3)t_v = C_{s,t,d}t_v$, де $C_{s,t,d}= 2(2m-1)(2p-v+1) = 2(2m-1)(2p-3)$ - часова складність помножувача для розширеного поля Галуа GF($d^m$).

Для випадку ($3p \le v$, $v = 4$) $p = 1$, що відповідає двійковим полям з характеристикою $d = 2$, затримка модифікованої комірки Гілда дорівнює $t_G=t_v$, а $t_{Mul} = (2n-1)t_G = (2n-1)t_v = C_{t,2}t_v$, де $C_{t,2} = 2n-1$ - часова складність помножувача для двійкового поля Галуа GF($2^n$).

2.10.4. Оцінювання часової складності помножувача з врахуванням структури комірок Гілда

У дослідженні [21] враховується внутрішня структура (рис. 2.4) модифікованої комірки Гілда і за базу для оцінювання часової складності та для визначення кількості елементів поля береться розширене двійкове поле Галуа GF($2^m$), тоді $d^m \approx 2^n$, $m \approx log_d 2^n = \frac{n}{log_2 d}$, часова складність для розширеного поля з характеристикою d $C_{t,d} = \frac{2(2n-1)(2\lceil log_2 d \rceil - v + 1)}{log_2 d}$. Відносно часової складності розширеного двійкового поля Галуа GF($2^m$) часова складності розширеного поля Галуа GF($d^n$) (відносна часова складність) $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$.

$R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - 3)}$ для v=4, . $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - 5)}$ для v=6. Якщо $R_{d,2} > 1$, то розширене поле з характеристикою d має меншу часову складність в порівнянні із розширеним двійковим полем. Як видно (рис. 2.9), перевагу перед двійковим полем мають поля з простими характеристиками GF($5^n$) та GF($7^n$) при використанні LUT6 з v=6 входами та поля GF($11^n$) та GF($13^n$) для LUT8 з v=8 входами.

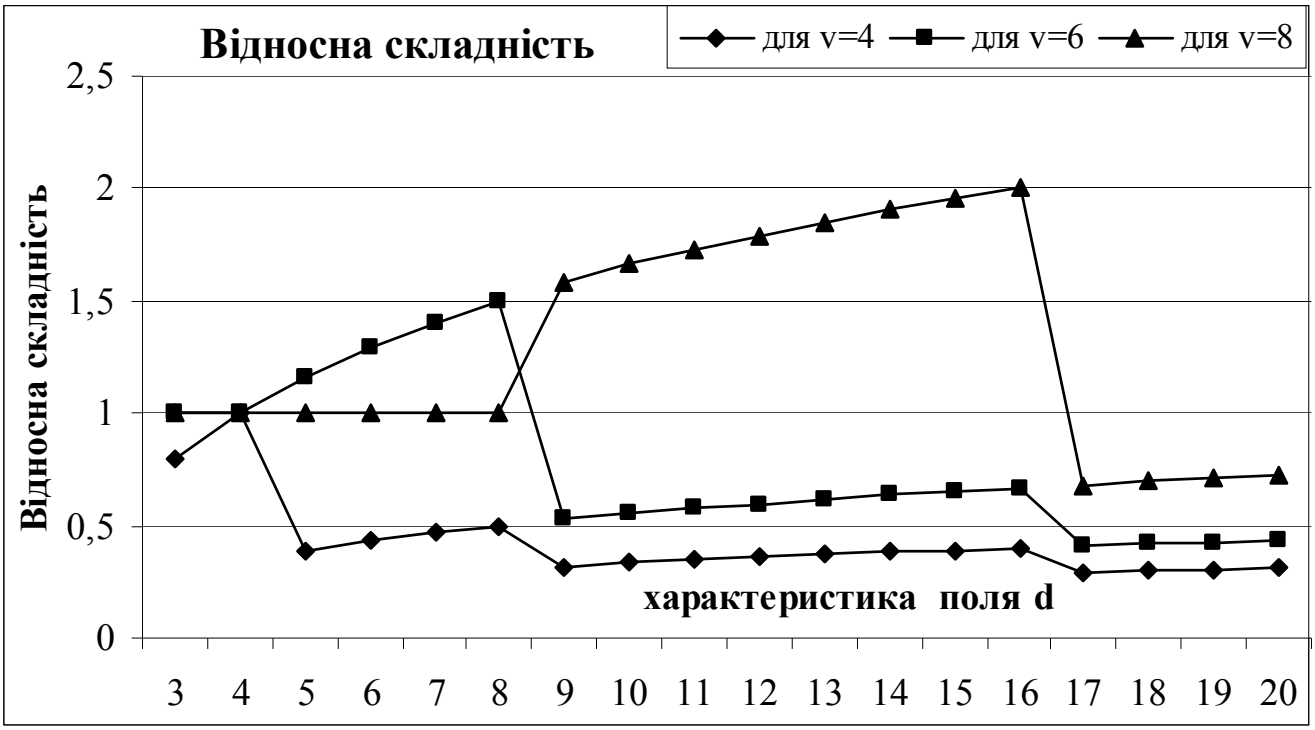



Рис. 2.9. Відносні часові складності з врахуванням структури комірки Гілда

Як видно, представлення внутрішньої структури комірки Гілда суттєво впливає на оцінку часової складності комірки та помножувачів на її основі.

У дослідженні [21] для множини розширених полів Галуа GF($d^m$) з приблизно однаковими кількостями елементів поля визначаються поля, у яких часова складність помножувача при його реалізації на сучасних ПЛІС є найменшою і меншою за часову складність помножувача для двійкового розширеного поля. Для аналізу обрано поліноміальний базис представлення елементів поля і матричний помножувач на основі модифікованих комірок Гілда. В залежності від представлення структури комірки Гілда та характеристик логічних вузлів (LUT) ПЛІС кращі часові характеристики можуть мати помножувачі для роботи у

розширених полях Галуа GF($d^m$) з характеристиками d=3, 5, 7. Зменшення часової складності при цьому по відношенню до часової складності для полів Галуа не перевищує 1,6 разів.

Запропонований метод оцінювання може бути застосовано при аналізі інших помножувачів, а також при аналізі помножувачів для полів з нормальним базисом представлення елементів поля.

2.11. Оцінювання структурної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ у нормальному та поліноміальному базисах

Порівняння структурної складності помножувачів для розширених полів Галуа з представленням їхніх елементів у поліноміальному та нормальному базисах у проаналізованих роботах не проводилося. Першим кроком може бути порівняння паралельних помножувачів, які одночасно формують усі розряди добутку, для двійкових полів Галуа $GF(2^m)$.

**Метою** досліджень [45], [71], [152], [75] є аналіз структурної складності паралельних помножувачів для двійкових полів Галуа $GF(2^m)$ з представленням їхніх елементів у поліноміальному та нормальному базисах для визначення найкращого базису і найкращого поля для побудови багатоядерних та багатосекційних помножувачів.

2.11.1. Послідовний помножувач для нормального базису розширених двійкових полів Галуа $GF(2^m)$

Структурну складність послідовних помножувачів для нормального базису можна оцінити [26] шляхом аналізу їхньої реалізації на умовній ПЛІС, кожний логічний елемент якої (квадрати на рис. 2.10, якому відповідає схема обчислення) може реалізувати довільну функцію двох змінних.

Структурну складність топології помножувача для нормального базису можна оцінити загальною довжиною $L$ з'єднань усередині квадратної області *Sqr* на рис. 2.10 (у [26] показано, що вузол згортки *Conv* дає незначний внесок до структурної складності помножувача): довжина горизонтального з'єднання $g_i$ у $i$-тому рядку дорівнює $g_i = x_i+1$, де $x_i$ - номер стовпця найправішої "1" в і-тому рядку,

вертикальна довжина з'єднання в *j*-му стовпці дорівнює $v_j=m+d_j+1$, де $d_j$ різниця номерів рядків у *j*-му стовпці з "1".

Кінцевий вираз:

$$L = \sum_{i=0}^{m-1}(g_i + v_i) \approx (1/2 \ldots 3/4)m^2 .$$

2.11.2. Оцінювання структурної складності паралельних помножувачів для нормального базису

Секційний помножувач (рис. 2.11) утворюється з послідовних помножувачів (секцій), кількість секцій *n* може бути від 1 (послідовний помножувач) до *m* (паралельний помножувач), усі секції однакового розміру і різняться циклічним зміщення по вертикалі і горизонталі суматорів і помножувачів у квадратній області (рис. 2.10) помножувальних матриць, що еквівалентно циклічному зсуву множників при обчисленні кожного наступного розряду добутку. Будемо вважати, що структурна складність помножувальних матриць не зменшується з-за циклічного зсуву їхніх елементів. Для спрощення будемо вважати, що секції розміщуються на кристалі у вигляді квадратної матриці максимальним розміром для паралельного помножувача *V=q*q* елементів, $q = \lceil \sqrt{m} \rceil$ .

Міжсекційні зв'язки розглядаємо як ще один додатковий «верхній» шар зв'язків, який лежить над квадратами *Sqr* та вузлами згортки *Conv*. Цей шар утворюють горизонтальні *B* та вертикальні *A* (рис. 2.11) зв'язки, які проходять від одного краю ПЛІС до другого, відповідно, зліва - направо і зверху - донизу.

Структурна складність *S* «верхнього» шару дорівнює сумарній довжині вертикальних і горизонтальних зв'язків, які проходять від краю до краю ПЛІС $S = V + G$,

де $V$ – структурна складність по вертикалі топології сигналів A та B;

$$V = (V_{Sqr} + V_{Conv})m + V_B ; \qquad V_{Sqr} = (L_{Sqr} \cdot H_{Sqr})m ; \qquad L_{Sqr} = m; H_{Sqr} = m ; \qquad V_{Conv} = L_{Conv} \cdot H_{Conv} ;$$

$$L_{Conv} = m ; \; HConv = level + 1 ;$$

$$V = m^3 + m^2 log_2 m + m \cdot q \cdot (m + log_2 m) = (m^2 + m \cdot q)(m + log_2 m) = m(m+q)(m + log_2 m) =$$

$$= m(m + \sqrt{m})(m + log_2 m) .$$

$V_{Sqr}$, $V_{Conv}$ – структурна складність проведення по вертикалі сигналів *A* «над» квадратною частиною секції та над її вузлом згортки;

$L_{Sqr}$, $H_{Sqr}$ – ширина та висота квадратної частини секції;

$L_{Conv}$, $H_{Conv}$ – ширина та висота вузла згортки секції;

$Level = log_2 m$ – рівень «глибини» згортки – кількість рядків логічних елементів ПЛІС за межами квадратної зони (рис. 2.10);

$V_B$ – структурна складність проведення по вертикалі сигналів B,

$V_B = m \cdot q \cdot (m + log_2 m)$,

*G* – структурна складність по горизонталі топології сигналів *B*, $G = m * m = m^2$.

Оскільки при такій моделі на нижньому шарі відсутні міжсекційні зв'язки, то його складність дорівнює складається усіх квадратів *Sqr* і зв'язаних із ним згорток *Conv*, а також складності виведення результатів $r_{ij}$ від кожної згортки до периферії кристалу ПЛІС.

Структурна складність «нижнього» шару *L* дорівнює складності *M* усіх помножувальних матриць $M_{i,j}$ (кожна з яких складається з квадратної частини $Sqr_{i,j}$ та вузла згортки $Conv_{i,j,}$ рис. 2.11):

$L = m \cdot M = km^3, k = ½ \ldots ¾$ .

При оцінюванні структурної складності потрібно також обчислити додаткові витрати на виведення результатів $r_{ij}$ з кожної матриці *M(i,j)* до периферії кристалу ПЛІС:

$r_{0j} = (q - 1) \cdot (m + level)$,

$r_{1j} = (q - 2) \cdot (m + level)$,

…

$r_{(q-1)j} = (q - q) \cdot (m + level) = 0$ .

Довжина всіх додаткових виводів:

$$R = \sum_{i=1}^{q} \sum_{j=0}^{q-1} r_{ij} = q(m + level) \sum_{i=1}^{q} (q - i) = q(m + level) \sum_{i=0}^{q-1} i = q(m + level) q(q - 1) / 2 =$$

$$= m(m + log_2 m)(\sqrt{m} - 1) / 2 .$$

Загальна структурна складність:

$C = L + S + R$,

$C = km^3 + m(m + log_2 m)(m + \sqrt{m}) + m^2 + m(m + log_2 m)(\sqrt{m} - 1)/2$.

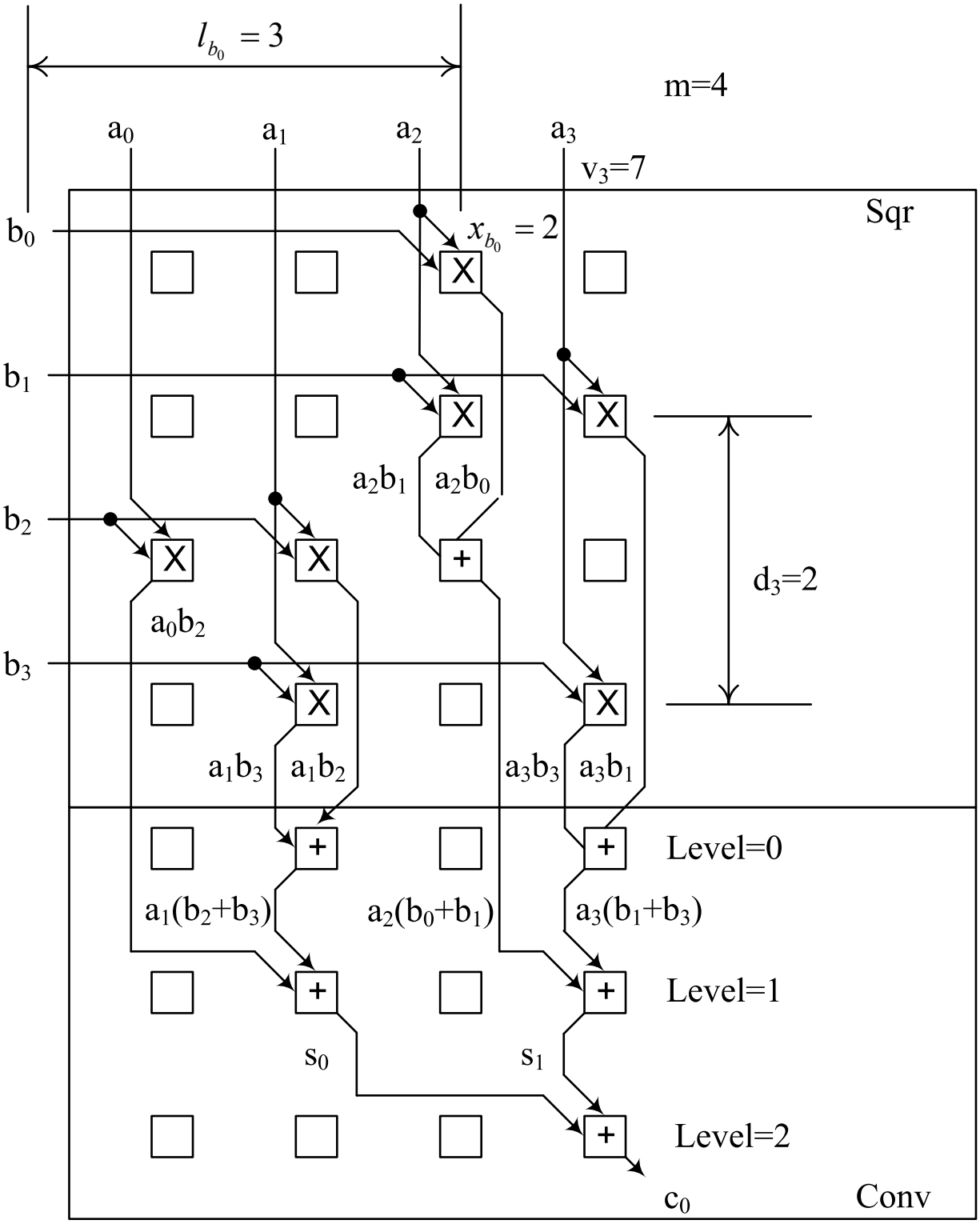



Рис. 2.10. Топологія умовної ПЛІС односекційного помножувача

Для великих *m* (*m* прямує до 1000) $C \approx (k+1)m^3, k = ½ \ldots ¾$.

Структурну складність паралельного помножувача для нормального базису двійкових полів Галуа $GF(2^m)$ можна оцінити як $O(m^3)$.

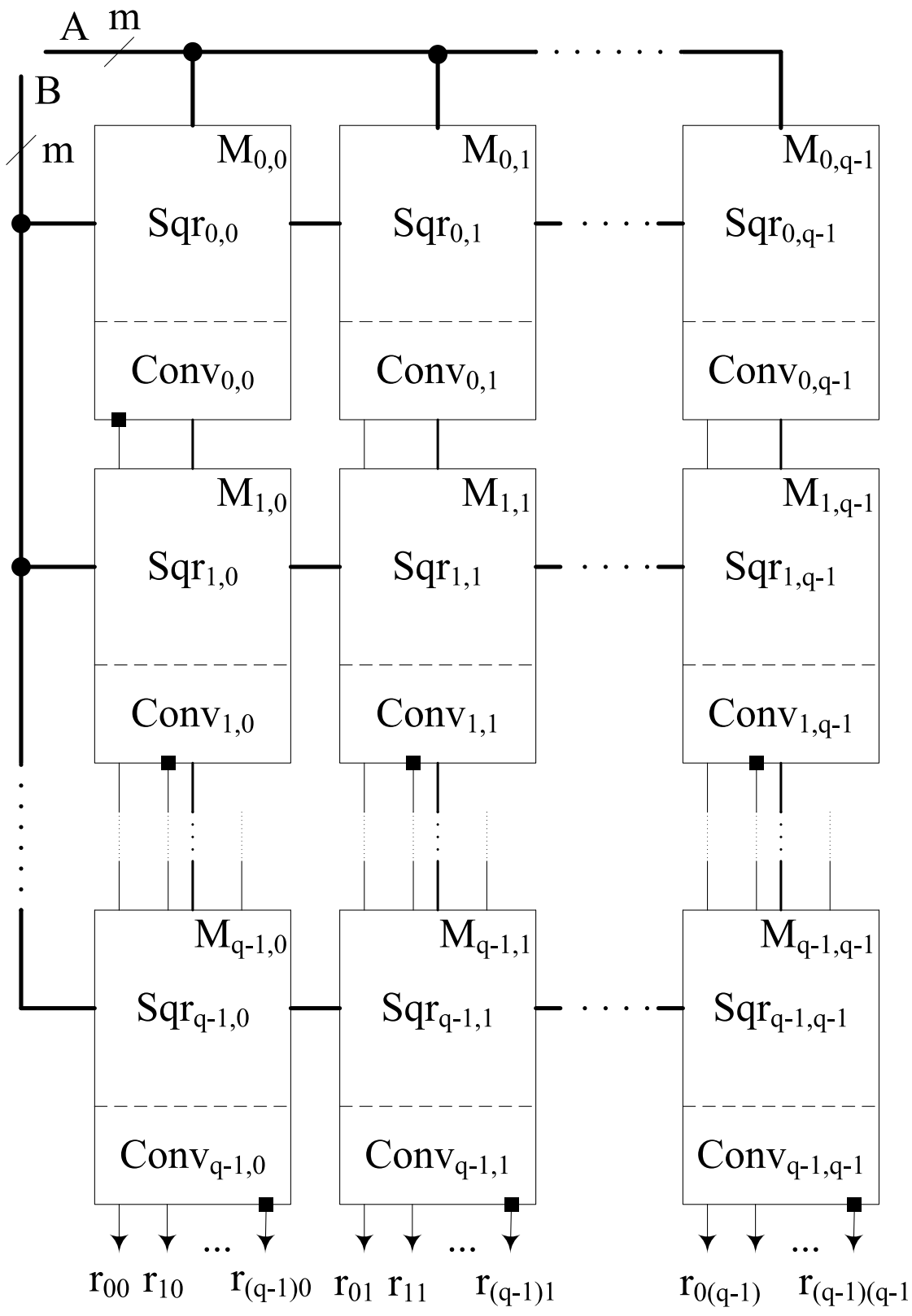



Рис. 2.11. Умовна топологія кристала багатосекційного помножувача

2.11.3. Паралельний помножувач для поліноміального базису.

Аналіз структурної складності паралельного помножувача для поліноміального базису будується на представленні топології з’єднань всередині

умовної ПЛІС двох сусідніх модифікованих комірок Гілда (рис. 2.12).

На рис. 2.5 показано функціональну схему помножувача двох елементів поля $GF(d^m)$ з використанням модифікованих комірок Гілда, детальну схему яких наведено на рис. 2.4. На рисунках позначено: $p_i$ – розряди утворюючого поле полінома, $p = \lceil log_2 d \rceil$ – кількість біт у записі числа $d$ (для двійкових полів Галуа $d = 2, p = 1$).

Пояснення до розрахунку структурної складності комірки Гілда для розширеного двійкового поля $GF(2^m)$ дає рис. 2.12.

Структурна складність $C_a$ топології сигналу $a$ через комірку Гілда дорівнює 2 (у комірці сигнал проходить повз 2 логічних елементи, один з них реалізує функцію множення, другий - додавання за модулем 2).

Структурна складність $C_b$ топології сигналу $b$ через комірку Гілда дорівнює 3 (у комірках сигнал проходить вниз повз 1 логічний елемент і проходить ліворуч повз 2 логічних елементи). Структурні складності топологій інших сигналів ($ab$, $c\_q$) всередині комірки дорівнює 1, оскільки вони всі проходять повз або через 1 логічний елемент. Сумарна структурна складність комірки Гілда $C_{Gd} = C_a + C_b + C_{ab} + C_{c\_q} = 7$.

Структурна складність $C_{PB}$ паралельного помножувача для поліноміального базису (рис. 2.5) складається з:

структурної складності всіх комірок Гілда $C_G = C_{Gd} \cdot m \cdot m \cdot 2 = 2C_{Gd} \cdot m^2 = 14m^2$;

структурної складності проведення вертикальних зв'язків між комірками Гілда: $C_V = C_S + C_f$,

$C_S$ – довжина зв'язків на вертикалі формування вихідних сигналів $S$, $C_S = 2m^2$;

$C_f$ - довжина вертикальних зв'язків, що використовуються для формування сигналів $f$: $C_f = 1 + 3 + 5 + \ldots + m - 2 = m(m - 1)/4$;

структурної складності $C_a$ проведення горизонтальних зв'язків $a$ до перших справа комірок Гілда, які використовують відповідний сигнал, у кожному рядку верхньої частини помножувача: $C_a = 2(1 + 2 + 3 + \ldots + (m - 1)) = m(m - 1)$

(«ширина» комірки Гілда дорівнює 2 одиницям структурної складності);

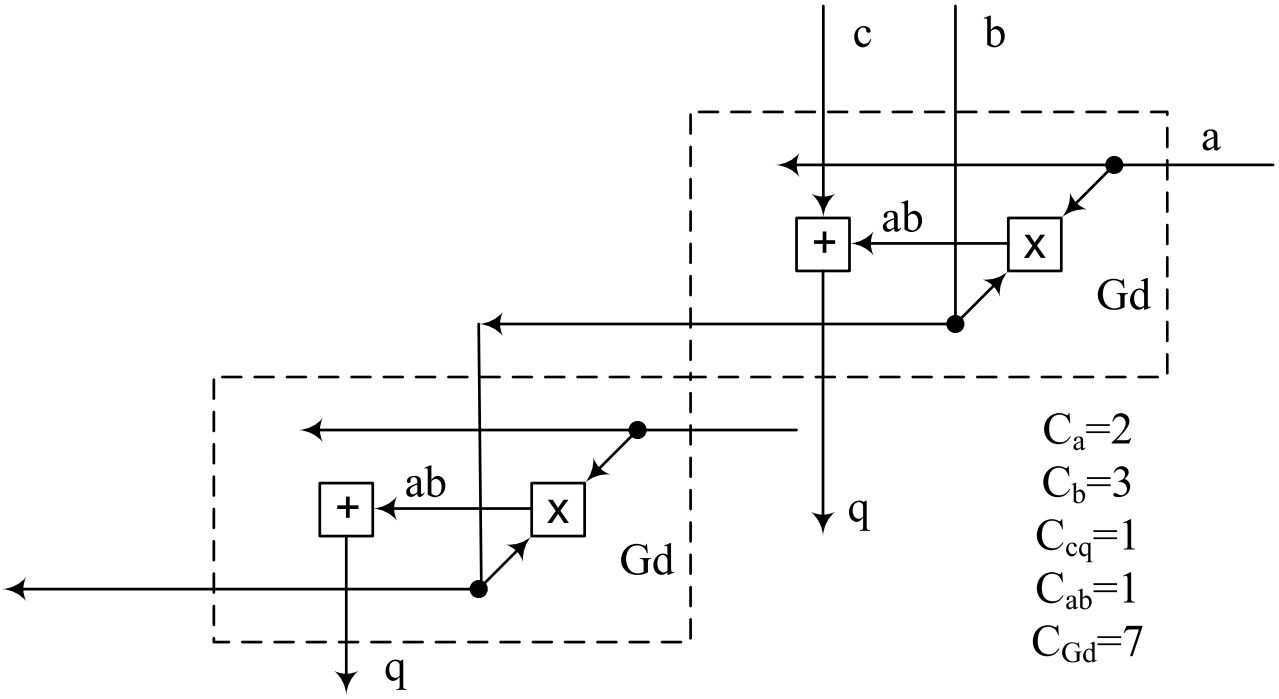



Рис. 2.12. Структурна складність комірки Гілда

структурної складності проведення горизонтальних зв'язків *f* між комірками Гілда: $C_f = m^2$;

структурної складності $C_p$ доведення розрядів $p_i$ утворюючого полінома до першої заправа комірки Гілда, яка використовує відповідний сигнал:

$$C_p = C_{p0} + C_{p1} + C_{p2} + \ldots + C_{p(m-1)} = 1*2 + 2*2 + 3*2 + \ldots + (m-1)*2 = m(m-1).$$

Загалом

$$C_{PB} = C_G + C_S + C_f + C_a + C_g + C_p = 14m^2 + 2m^2 + m(m-1)/4 + + m(m-1) + m^2 + m(m-1) =$$

$$= 19m^2 + m(m-1)/4 - 2m .$$

Для великих *m* (*m* прямує до 1000) $C_{PB} \approx 20m^2$.

Структурну складність паралельного помножувача для поліноміального базису двійкових полів Галуа $GF(2^m)$ можна оцінити як $O(m^2)$.

2.11.4. Порівняння структурної складності помножувачів

Результати порівняння структурної складності помножувачів для поліноміального та нормального базисів показано на рис. 2.13, рис. 2.14 та рис. 2.15.

Для степенів $m < 12$ (рис. 2.13) двійкових полів Галуа $GF(2^m)$ меншу структурну складність мають помножувачі для роботи у нормальному базисі. Для

більших степенів (рис. 2.14) меншу структурну складність мають помножувачі для роботи у поліноміальному базисі. Для $m >> 12$ (рис. 2.15, за [93] $m \geq 163$) використання поліноміального базису дає зменшення структурної складності в порівнянні з нормальним базисом приблизно в $m$ разів.

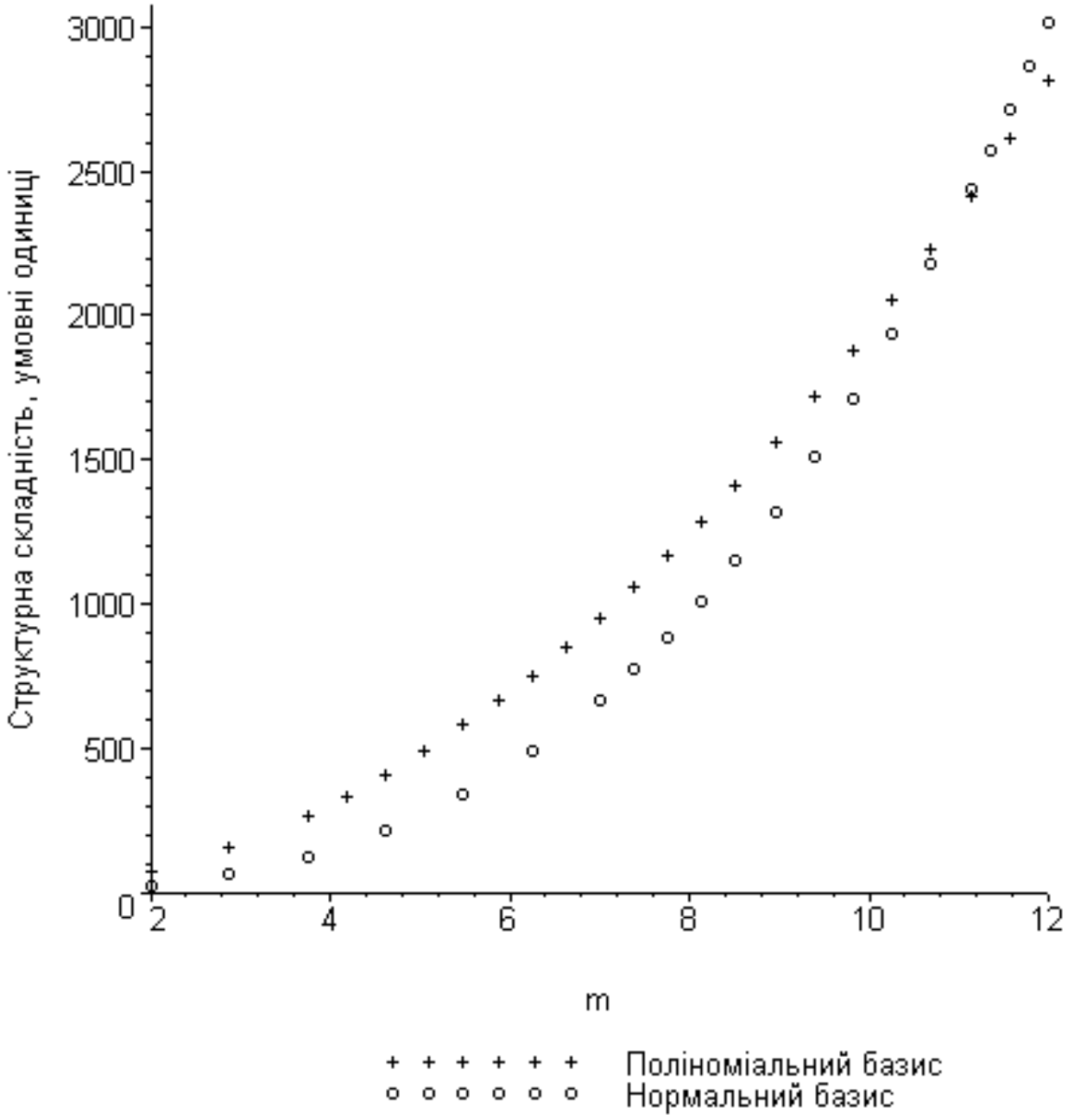



Рис. 2.13. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 12$)

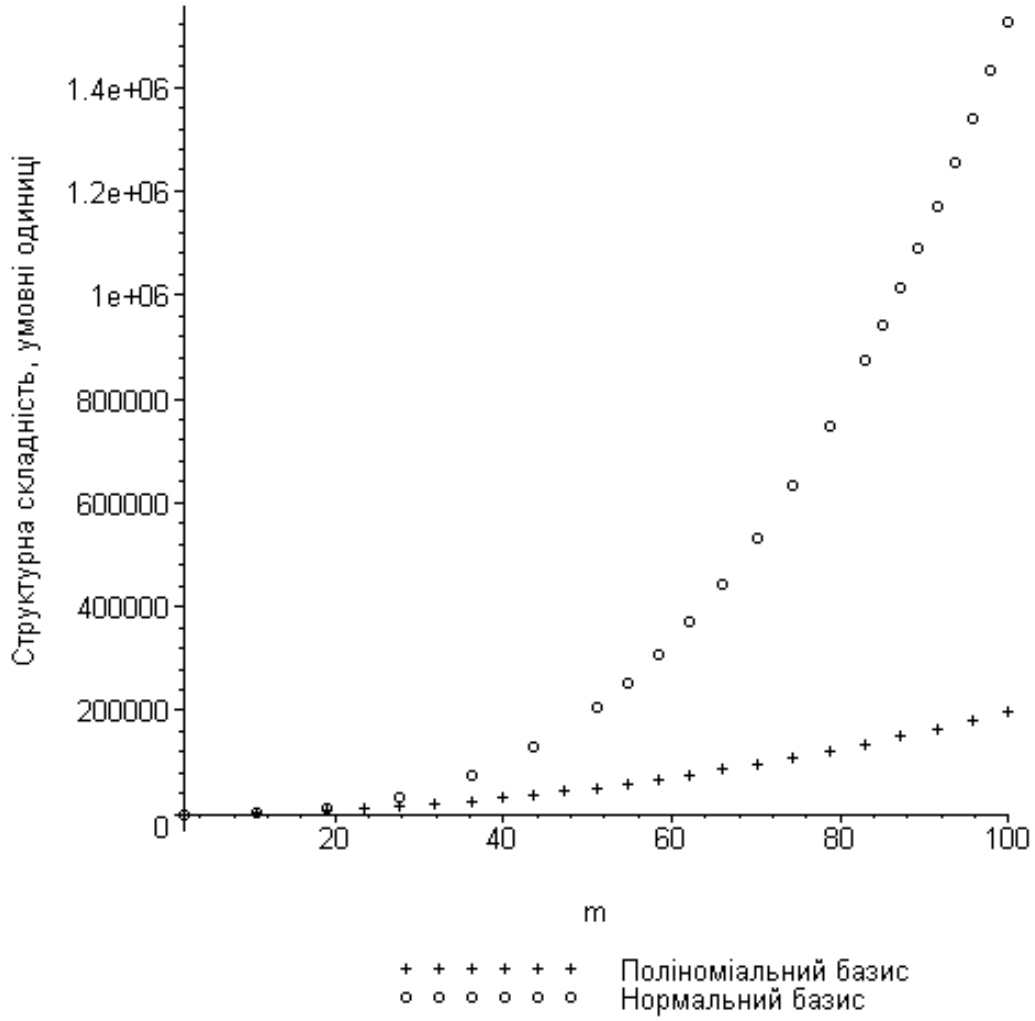



Рис. 2.14. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 100$)

Більша структурна складність помножувачів для нормального базису ускладнює і робить неможливим створення їхніх багатосекційних та паралельних версій [20]. Менша структурна складність помножувачів для поліноміального базису дозволить створити їхні багатосекційні версії з більшою кількістю секцій (з більшим рівнем паралелізму і, відповідно, більшою продуктивністю) ніж у аналогічних помножувачів для нормального базису.

## 2.12. Оцінювання ємнісної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$

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. На оцінюванні

довжини цих кодів будується метод оцінювання ємнісної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$.

Довжина коду одного елемента розширеного двійкового поля $GF(2^{998})$ дорівнює 998 біт. Для полів $GF(d^m)$ з порядком $d^m \approx 2^{998}$ довжина коду елемента $LC = m/\lceil \log_2 d \rceil$ (таблиці 2.8, рис. 2.16 та рис. 2.17), 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 $p \approx 2^{998}$).

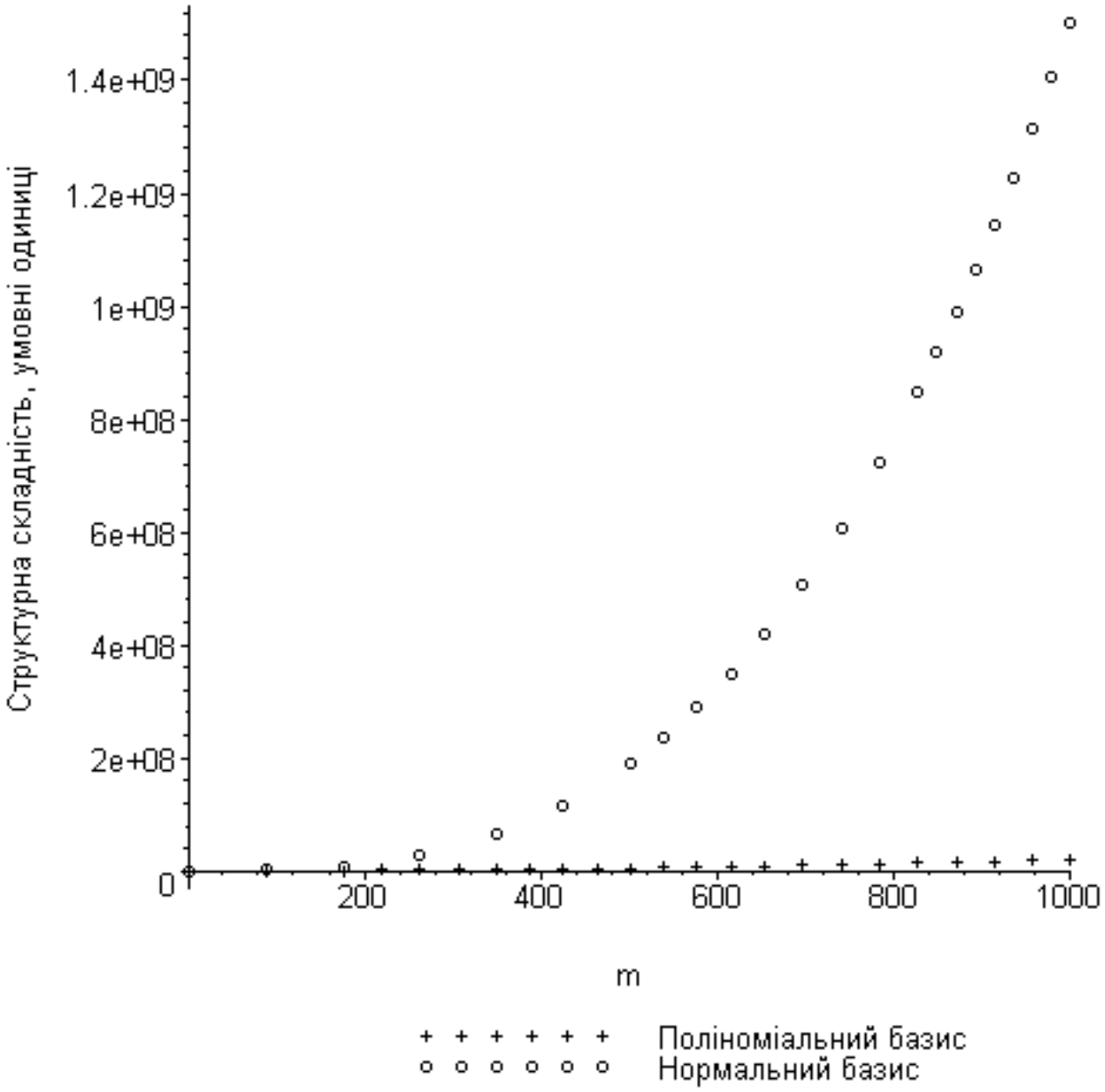



Рис. 2.15. Структурна складність помножувачів для поліноміального та нормального базисів ($m < 1000$)

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 точки зору ємнісної складності найкраще використовувати двійкові та прості поля Галуа, але використання інших полів не приведе до збільшення довжина кодів (ємнісної складності) більше ніж на 30 % [73].

2.12.1. Оцінка програмно-часової складності Сп помножувачів для поліноміального базису

Одним з методів злому системи криптографічної інформаційної безпеки є метод грубої сили [197], в якому комп'ютер загального призначення вибирає всілякі ключі або паролі, доки один з них не підійде. При цьому під час злому виконуються ті самі операції над елементами полів Галуа, що і в апаратних криптопроцесорах. Для комп'ютерів загального призначення необхідно оцінити відносну програмно-часову складність через час виконання основної операції при зломі - час множення елементів полів Галуа для розширених полів з різними основами, але з приблизно однаковою кількістю елементів поля [152], [153], [159].

Основою для порівняння результатів було взято поле GF($2^{999}$). Це поле рекомендовано стандартним [191]. Розрахунки проводились за допомогою пакету Maple 2017 [195]. Під час перевірки часової складності 5 разів було проведено вимірювання часу виконання 10 000 операцій множення елементів кожного з полів GF($d^m$), обраного для тестування. Поля були вибрані так, щоб для них виконувалася умова $2^{999} \approx d^m$ (d - просте ціле число, m - ціле число), тобто поля мали приблизно однакову кількість елементів. Середнє значення часу було розраховано після 5 експериментів. Також визначалася відносна часова складність співвідношенням часу множення в поле GF($d^m$) до часу множення в полі GF($2^{999}$).Час виконання такої кількості множення відносно часу виконання того ж числа операцій у двійковому полі GF($2^{999}$) наведено в таблиці 2.6 та таблиці 2.7 та на рис. 2.18. Таблиця 2.6 показує час множення в полі GF($2^{999}$) з польовим поліномом, рекомендованим [191], і поліномом поля, який було знайдено за допомогою пакету Maple.

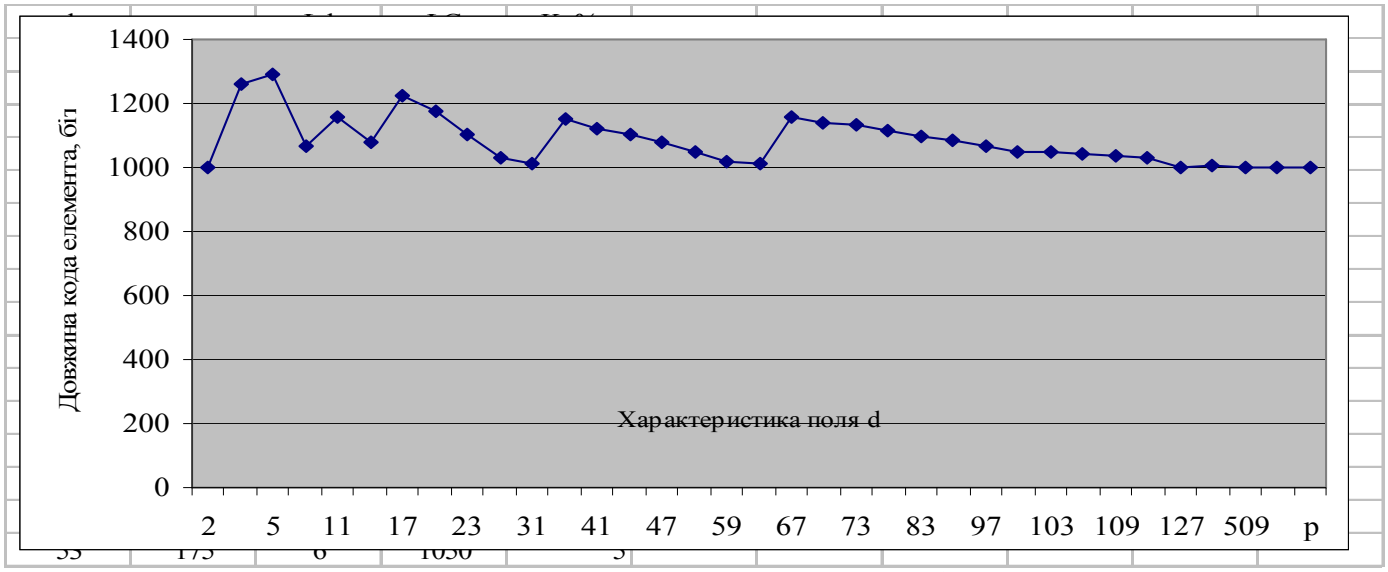



Рис. 2.16. Довжина кодів елементів полів GF($d^m$) в бітах


Рис. 2.17. Відносні довжини кодів елементів полів GF($d^m$), в процентах

## 2.13. Метод оцінювання складності злому апаратних засобів КЗІ

*Таблиця 2.6*

**Часова складність множення в двійковому поле Галуа, с**

| Field Base | 1 | 2 | 3 | 4 | 5 | Polynomial |
|---|---|---|---|---|---|---|
| 2 | 5,30 | 5,42 | 5,25 | 5,38 | 5,27 | IEEE |
| 2 | 5,67 | 5,77 | 5,61 | 5,83 | 5,55 | Maple |

*Таблиця 2.7*

**Часова складність множення в полях Галуа**

| Характеристика поля | Відносний час |
|---|---|
| 2 | 1,00 |
| 3 | 1,46 |
| 5 | 1,18 |
| 7 | 0,84 |
| 11 | 0,59 |
| 13 | 0,53 |
| 17 | 0,45 |
| 19 | 0,42 |
| 23 | 0,38 |
| 29 | 0,33 |
| … | … |
| $p_i \approx 2^{768}$ | 0,03 |
| p | 0,03 |

*Таблиця 2.8*

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

| d | m | Ld | LC | K, % | d | m | Ld | LC | K, % |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 998 | 1 | 998 | 0 | 67 | 165 | 7 | 1155 | 16 |
| 3 | 630 | 2 | 1260 | 26 | 71 | 163 | 7 | 1141 | 14 |
| 5 | 430 | 3 | 1290 | 29 | 73 | 162 | 7 | 1134 | 14 |
| 7 | 356 | 3 | 1068 | 7 | 79 | 159 | 7 | 1113 | 12 |
| 11 | 289 | 4 | 1156 | 16 | 83 | 157 | 7 | 1099 | 10 |
| 13 | 270 | 4 | 1080 | 8 | 89 | 155 | 7 | 1085 | 9 |
| 17 | 245 | 5 | 1225 | 23 | 97 | 152 | 7 | 1064 | 7 |
| 19 | 235 | 5 | 1175 | 18 | 101 | 150 | 7 | 1050 | 5 |
| 23 | 221 | 5 | 1105 | 11 | 103 | 150 | 7 | 1050 | 5 |
| 29 | 206 | 5 | 1030 | 3 | 107 | 149 | 7 | 1043 | 5 |
| 31 | 202 | 5 | 1010 | 1 | 109 | 148 | 7 | 1036 | 4 |
| 37 | 192 | 6 | 1152 | 15 | 113 | 147 | 7 | 1029 | 3 |
| 41 | 187 | 6 | 1122 | 12 | 127 | 143 | 7 | 1001 | 0 |
| 43 | 184 | 6 | 1104 | 11 | 251 | 126 | 8 | 1008 | 1 |
| 47 | 180 | 6 | 1080 | 8 | 509 | 111 | 9 | 999 | 0 |
| 53 | 175 | 6 | 1050 | 5 | 1021 | 100 | 10 | 1000 | 0 |
| 59 | 170 | 6 | 1020 | 2 | p | 1 | 998 | 998 | 0 |
| 61 | 169 | 6 | 1014 | 2 | | | | | |

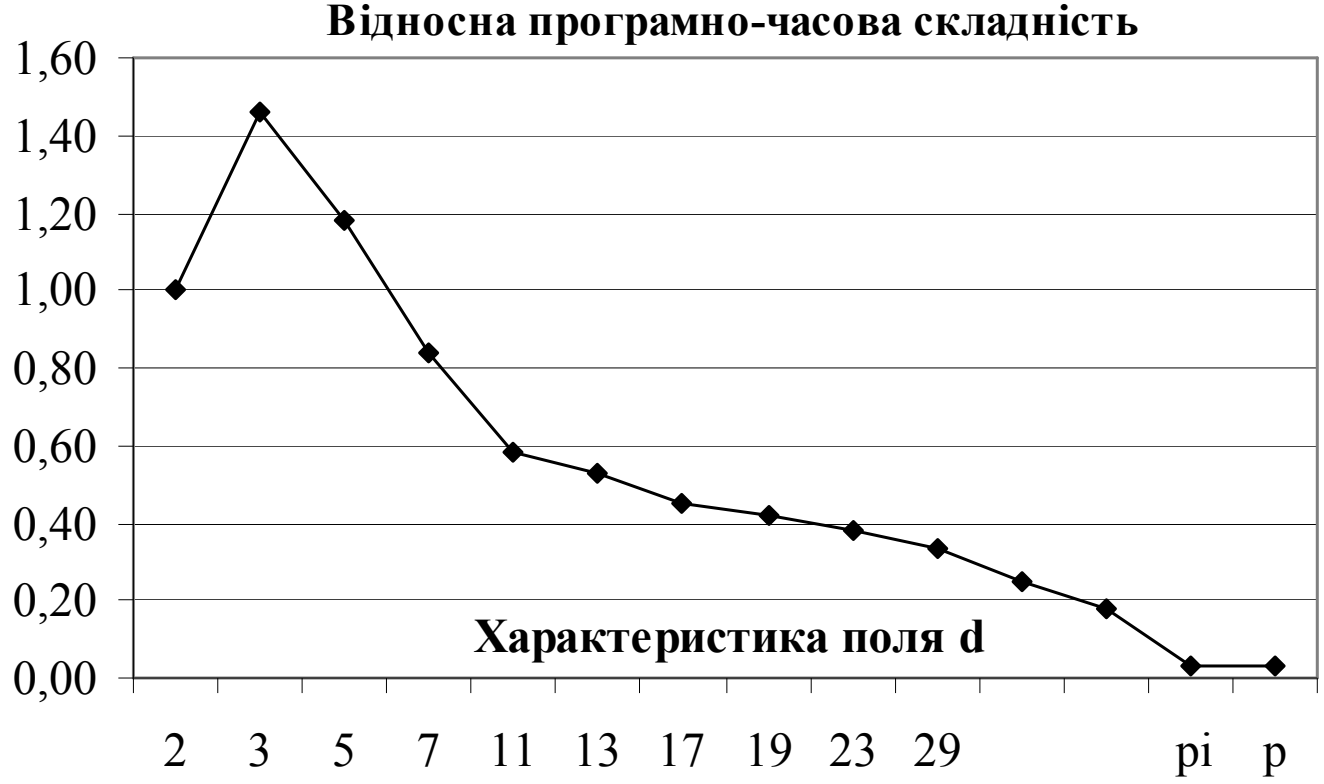



Рис. 2.18. Відносна програмно-часова складність Са множення в розширених полях Галуа

Як видно з таблиці 2.6, час виконання операцій у цих двох випадках різниться несуттєво. Тому всі дослідження були продовжені для поліномів, які було знайдено за допомогою пакету Maple. Аналогічне дослідження також проводилося для простого поля $GF(p^1)$, де p - найближче просте число, яке перевищує $2^{999}$. Як видно з таблиці 2.7, програмне множення елементів трійкового розширеного поля має найдовший час виконання. Це забезпечує апаратні криптопроцесори на базі таких полів додатковим захистом від злому. Особливе положення трійкових полів підтверджується приміткою в стандарті [98]: «Випадок p=3 (p – просте число, характеристика поля, примітка автора) не розглядається в цьому стандарті для простоти, а не з міркувань безпеки». Операції, що виконуються програмним забезпеченням на елементах простих полів, виконуються найшвидше, що вказує на недоцільність побудови апаратних криптографічних процесорів на основі таких полів.

Програмне множення в двійкових полях має одну з найвищих часових складностей, воно посідає третє місце після множення в полях з характеристиками 3

і 5. Тому наступне дослідження, в основному, зосереджуватиметься на створенні апаратних засобів КЗІ, які оперують з елементами двійкових полів Галуа.

Програмне множення у полі з характеристикою $p_i \approx 2^{768}$, яке використовуються в постквантовій криптографії на основі ізогеній еліптичних кривих (таблиця 2.9) 117], виконується в 30 разів швидше, ніж у двійкові полях з $p$=2.

*Таблиця 2.9.*

**Типи криптоперетворень, що є стійкими до квантового криптоаналізу**

| | |
|---|---|
| Використання решета числового поля (Lattice-based primitives) | Криптографічна стійкість (безпека) залежить від складності розв'язання рівняння на алгебраїчних решітках |
| Мультиваріативні перетворення (Multi-variate primitives) | Криптографічна стійкість (безпека) залежить від складності рішення системи багатовимірних по-ліноміальних рівнянь |
| Використання алгебраїчних кодів (Code-based primitives) | Криптографічна стійкість (безпека) залежить від складності виконання завдання декодування лі-нійного коду |
| Асиметрична криптографія на гешах (Hash-based primitives) | Криптографічна стійкість (безпека)а залежить від складності знаходження колізій або прообразів в криптографічних геш-функцій |
| Використання ізогеній еліптичних кри-вих (Isogenies-based key primitives) | Криптографічна стійкість (безпека) залежить від складності знаходження невідомої ізогенії між парою суперсингулярних еліптичних кривих |

2.13.1. Оцінка апаратно-часової складності Са помножувачів у полях Галуа

Реалізовані в ПЛІС апаратні помножувачі для розширених полів Галуа $GF(d^m)$ з приблизно однаковою кількістю елементів $d^m \approx 2^n$ аналізуються з точки зору їх часової складності для визначення полів ([44], [70]). Відносно $GF(2^n)$ результати оцінки наведено на рис. 2.

2.13.2. Оцінка часової складності апаратного захисту інформації і програмного злому захисту Сз = Сп/Са.

Припустимо, що апаратна реалізація використовується користувачами засобів захисту даних, а програмна - зловмисниками. Тоді можна ввести узагальнений індекс часової складності програмно-апаратної реалізації. Обчислимо цей показник як відношення часової складності програмної реалізації до часової складності апаратної реалізації для тих самих полів Сз = Сп/Са. Коли значення цього показника більше, зловмисники будуть мати більше проблем, тому захист даних буде кращим.

Результати оцінки апаратно-програмної складності показано на рис. 2.20.

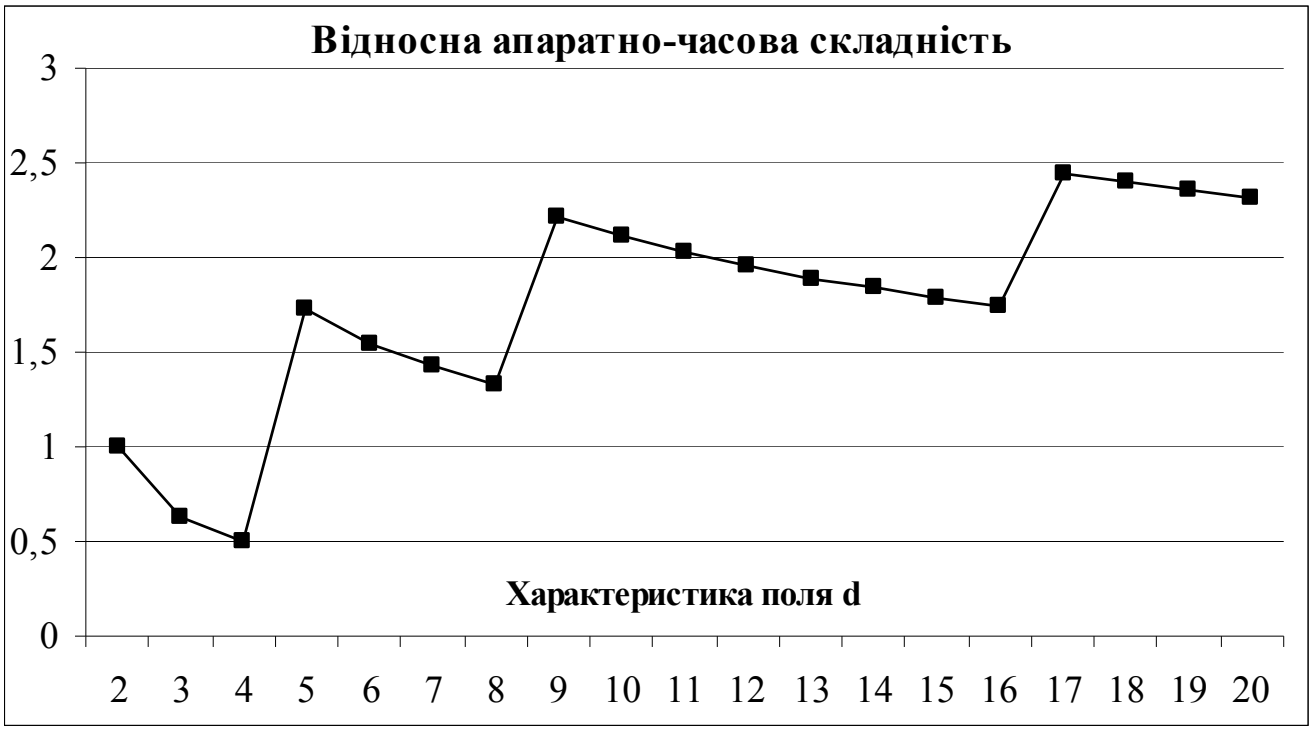



Рис. 2.19. Відносна апаратно-часова складність Са множення в розширених полях Галуа

Як видно з рис. 2.20, трійкові та двійкові поля Галуа забезпечують найкращий захист даних. Поля з більшими характеристиками забезпечують слабший захист. Використання апаратних засобів для роботи у таких полях має менший ефект, ніж для роботи в двійкових і трійкових полях. Як результат, використання апаратних засобів для роботи в полі з характеристикою $d=2^{768}$ [117] також має менший ефект, ніж для роботи в двійкових і трійкових полях.

Використання ізогеній суперсингулярних еліптичних кривих орієнтовано на використання полів Галуа з великими характеристиками, тому їх орієнтовано на використання програмну реалізацію.

Висновок: з проведених досліджень ємнісної, структурної та часової складності помножувачів елементів розширених полів Галуа з приблизно однаковим порядком, а також з врахуванням відомих результатів оцінювання апаратної складності помножувачів, видно, що найкращими полями для побудови апаратних помножувачів є трійкове та двійкове розширені поля Галуа, а також поля з характеристиками 5 та 7.

Складність криптоаналізу криптосистеми на основі ізогеній суперсингулярних

кривих, що працює в полі $GF(p^m)$, з використанням квантових комп'ютерів складає $O(\sqrt[9]{p})$ [117]. Для збільшення стійкості необхідно збільшувати $p$, що зменшує ефективність апаратної реалізації і збільшує ефективність програмних реалізацій.


Рис. 2.20. Відносна складність злому у різних полях Сз = Сп/Са

2.14. Вдосконалений метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

2.14.1. Надлишковість кодів елементів розширених полів Галуа $GF(d^m)$

На відміну від двійкових полів Галуа $GF(2^m)$ у розширених поля $GF(d^m)$ з іншою основою $d > 2$ коди елементів мають надлишковість, яку можна використати для вдосконалення відомих методів вбудованого тестування.

Кожний розряд коду елемента розширеного поля Галуа $GF(d^m)$ представляється $n_b = \lceil \log_2 d \rceil$ бітами, за допомогою яких можна закодувати $d_t = 2^{\lceil \log_2 d \rceil} \geq d$ різних кодових комбінацій. При цьому залишається $d_d = d_t - d$ кодових комбінацій, які ніколи не будуть зустрічатися при опрацюванні елементів полів Галуа 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 (вбудованого тестування) [43]. Ознакою помилки є поява будь-якої забороненої комбінації в будь-якому розряді коду будь-якого елемента поля Галуа.

Наприклад, для трійкового поля Галуа GF($3^m$) код кожного розряду $a_i$ його елемента (рис. 2.2) може мати значення, які містить таблиця 2.10.

*Таблиця 2.10*

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

| $a_i$ | 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 |

Якість контролю (тестопридатність) 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 тестопридатності різних розширених полів Галуа наведено у таблиці 2.11 та рис. 2.21. Також можна оцінити зважену тестопридатність $q_d = 100*d_d/(dn_b)$ для полів, які мають заборонені значення кодів, рис. 2.22), як попереднє значення ділене на кількість біт, які необхідно аналізувати для визначення заборонених комбінацій.

Для збільшення тестопридатності рекомендується використовувати поля з характеристикою d, яка є першим простим числом більшим за степінь 2, наприклад, d = 5. Найменшу тестопридатність мають поля 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 забезпечення тестопридатності, 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 тестопридатності 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 2.11 та Рис. 2.21 необхідно 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)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.

2.14.2. Визначення способів формування ознак помилки опрацювання елементів розширених полів Галуа

Деякі можливі варіанти розміщення дозволених і заборонених кодів серед усіх кодів розрядів елементів полів Галуа представлено на рис. 2.22. Повний діапазон кодів – це діапазон від $00..0_2$ до $11..1_2$. Дозволені та заборонені коди серед них можуть бути розміщено групами (рис. 2.22) 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. 2.22, а), на початку (рис. 2.22, б); в середині (рис. 2.22, в), та по краях (рис. 2.22, 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 $Error_i$.

Запропоновано табличний спосіб опису ознаки виникнення помилкових кодів. 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 [19].

*Таблиця 2.11*

**Тестопридатність полів GF($d^m$)**

| d | $q_t$ | q | log2d | $\lceil \log_2 d \rceil$ | $d_t$ | $d_d$ |
|---|---|---|---|---|---|---|
| 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 |

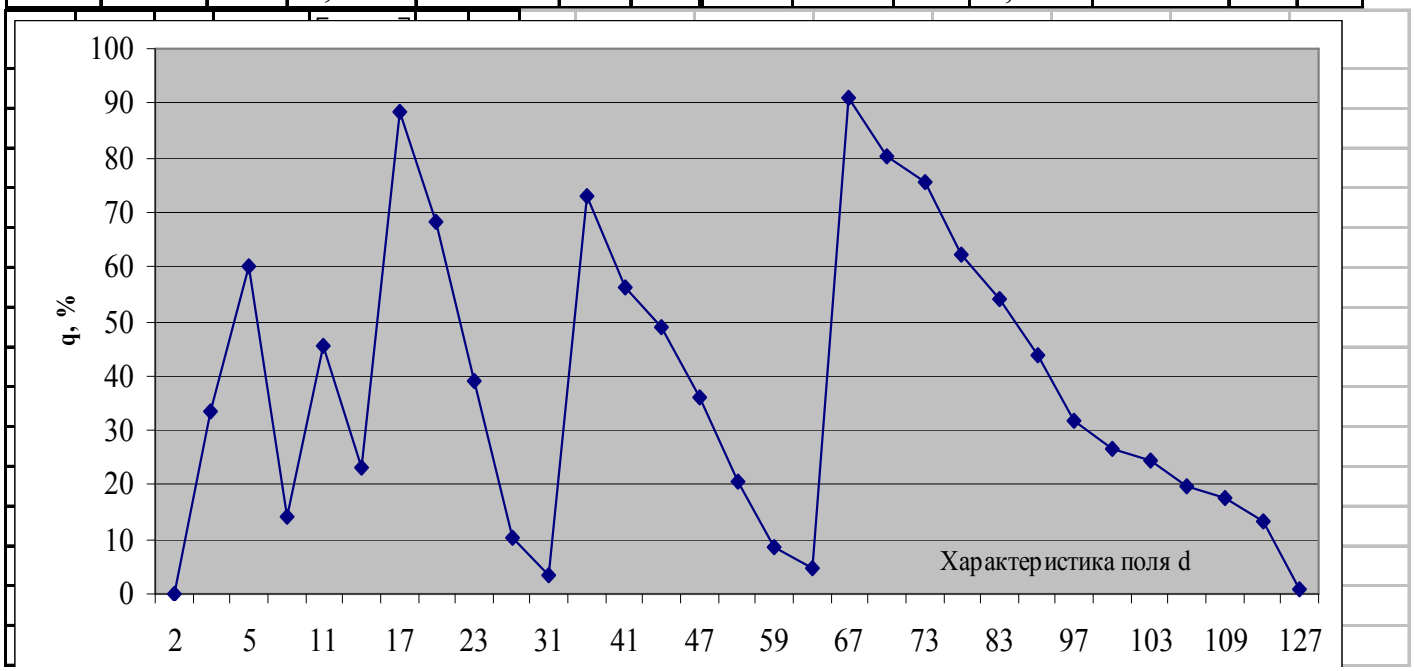



Рис. 2.21. Тестопридатність полів GF($d^m$), %

Наприклад (табл. 2.12) 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 $A_0, A_1, A_2$.

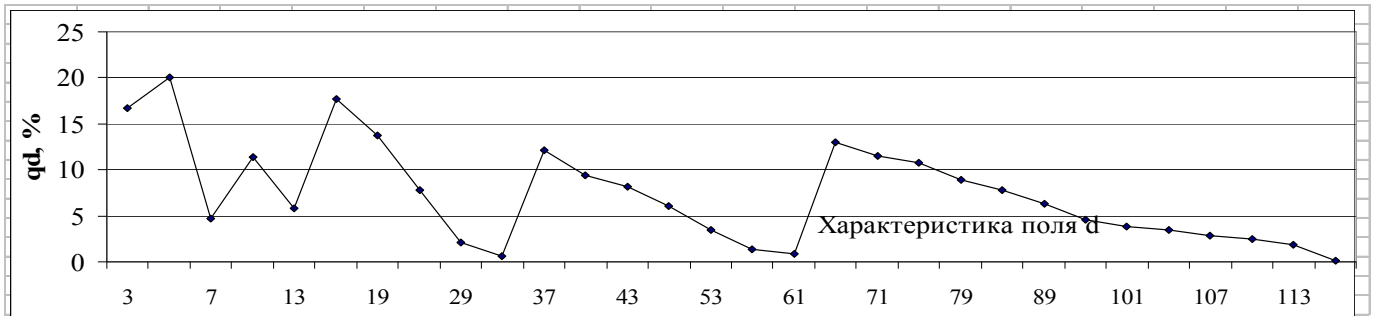



Рис. 2.22. Зважена тестопридатність полів GF($d^m$), %

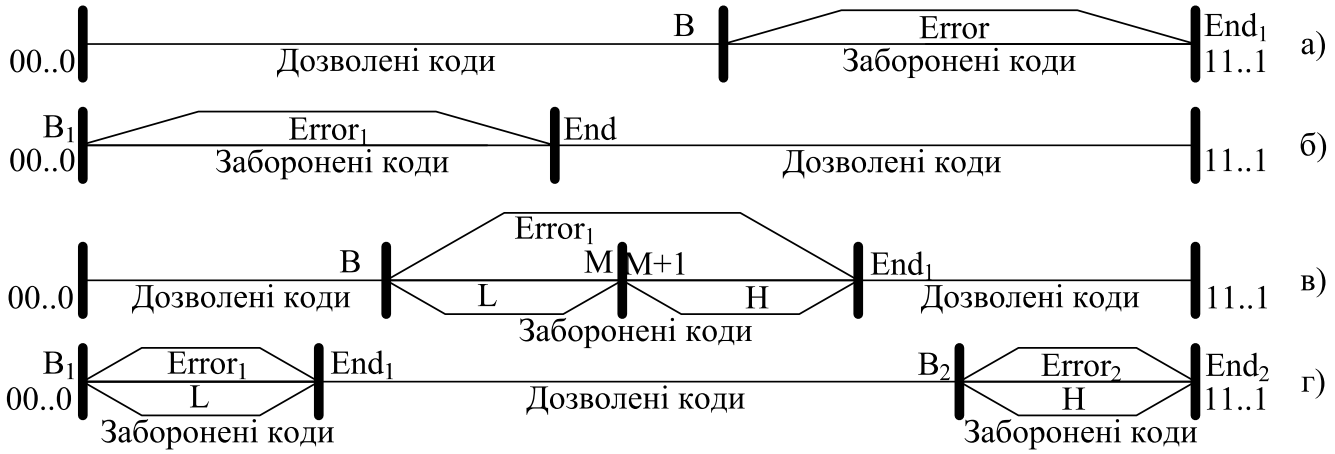



Рис. 2.23. Дозволені і заборонені коди розрядів елементів полів Галуа *GF($d^m$)*

Розряди змінної групи перебігають всі можливі значення від 000 до 111. Тому їх можна спростити і записати загальний вираз для всіх заданих у табл. 2.12) наборів, тобто, для наведеного діапазону кодів $Error_1 = A_7 \overline{A_6} A_5 A_4 A_3$.

*Таблиця 2.12*

**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** | - | - | - |

У більш складних випадках описаний принцип використовується послідовно. Наприклад, для діапазону заборонених кодів 1E3A4...04B8F, які знаходяться всередині повного діапазону кодів, таблицю мінімізації наведено в табл. 2.13 (показано формування сигналу Error1) та табл. 2.14 (формування сигналу Error2).

Рядок I0 (табл. 2.13) кодує початковий код діапазону - 4B8F. Оскільки його код має в кінці 1, то він в даному 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 *I1*.

Останній код, який кодує рядок *I1*, дорівнює 4B9F. Він менший за верхню границю діапазону (1E3A4), і тому перевіряється наступний код - 4BA0. Так як він закінчується п'ятьма двійковими 0, то можна ці п'ять розрядів виділити у змінну групу і мінімізувати, як це зроблено в рядку *I2*.

Останній код, який кодує рядок *I2*, 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 *I3*.

Аналогічні дії виконуються до рядка *I7* включно.

Останній код, який кодує рядок I8, 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 незначних подальших скорочень (використовується формула поглинання $a\bar{b} \vee b = a \vee b$ - зникають закреслені 0 у табл. 2.13):

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

Подібним чином створюється таблиця мінімізації старшої частини діапазону заборонених кодів (табл. 2.14) та формується сигнал $Error_2$.

На відміну від попередньої таблиці рух відбувається в зворотному напрямі: від верхньої границі до середньої точки (*M* на рис. 2.22, в).

Рядок *I0* кодує кінцевий код діапазону - 1E3A4. Оскільки закінчується 0, то в даному 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 *I1*.

Перший код, який кодує рядок *I1*, 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 *I2*.

Аналогічні дії можна виконувати до рядка *I8* включно.

*Таблиця 2.13*

**Мінімізація діапазону кодів в напрямку зростання кодів**

| N | Розряди коду A | | | | | | | | | | | | | | | | Диапазон кодів | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $A_{16}$ | $A_{15}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_9$ | $A_8$ | $A_7$ | $A_6$ | $A_5$ | $A_4$ | $A_3$ | $A_2$ | $A_1$ | $A_0$ | 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 2.14*

| N | Входи A ПЛМ | | | | | | | | | | | | | | | | Диапазон кодів | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $A_{16}$ | $A_{15}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_9$ | $A_8$ | $A_7$ | $A_6$ | $A_5$ | $A_4$ | $A_3$ | $A_2$ | $A_1$ | $A_0$ | 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 I9, дорівнює 00000. Він менший за нижню границю діапазону, тому цей рядок є зайвим і з подальшого розгляду вилучається: $Error_2 = I_0 \vee I_1 \vee \ldots \vee I_8 = A_{16}\overline{A_{12}}\,\overline{A_{11}}\,\overline{A_{10}}\,\overline{A_6}\,\overline{A_4}\,\overline{A_3}\,\overline{A_1}\,\overline{A_0} \vee A_{16}\overline{A_{12}}\,\overline{A_{11}}\,\overline{A_{10}}\,\overline{A_6}\,\overline{A_4}\,\overline{A_3}\,\overline{A_2} \vee \ldots \vee A_{16}\overline{A_{15}}$. Тут також виконано додаткове спрощення (використовується формула поглинання $a\bar{b} \vee b = a \vee b$ - зникають закреслені 1 у табл. 2.13).

Таблиці мінімізації для інших варіантів розміщення заборонених кодів (рис. 2.22) 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. 2.13 та табл. 2.14 приймається приблизно рівною кількості двійкових розрядів $n_b = \lceil log_2 d \rceil$ коду, що мінімізується - $N_r \approx n_b = \lceil log_2 d \rceil$;

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 $GF(d^m)$ $HC_1=N_rN_b=n_b^2/2=\lceil log_2 d \rceil^2/2$.

Таким чином, 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 з характеристиками $d$, які є або степенем 2 ($d = 2$), або є 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 $d$.

## 2.15. Метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі

Операційні пристрої (в порівнянні з пристроями керування) мають більшу розрядність, споживають більше потужності і характеризуються більшим електромагнітним випромінюванням. Їхнє маскування є більш важливим і методи його реалізації описано в літературі. Відомі методи розширено для операцій знаходження обернених елементів у розширених полях Галуа $GF(2^m)$.

Сьогодні математичною основою для обробки цифрового підпису є еліптичні криві [93]. У цьому випадку обробка точок еліптичної кривої базується на операціях над елементами поля Галуа $GF(2^m)$, $m \leq 1000$ - це число бітів у коді [191], елементи поля можна представити в поліноміальному та нормальному базах. Апаратна реалізація процесорів для опрацювання елементів полів Галуа в ПЛІС, яка повинна

виконувати паралельне множення та ділення таких гігантських кодів для згаданих задач і полів, вимагає великих витрат на обладнання. При цьому здійснюється одночасне перемикання великої кількості елементів, що може демаскувати роботу пристрою.

У полях Галуа частка α/β може бути обчислена безпосередньо (за допомогою алгоритму з входами α та β) або опосередковано (шляхом обчислення мультиплікативної інверсії (оберненого елемента, зворотного елемента) $\beta^{-1}$, а потім множення його на α у процесорах для опрацювання елементів полів Галуа. Існує два поширені методи для ділення у двійкових полях Галуа $GF(2^m)$, прямий (далі - Метод 1 у р. 3.4) і непрямий [191]. Прямий метод є розширеним алгоритмом Евкліда. Розширений алгоритм Евкліда використовується у поліноміальному базисі $GF(2^m)$ [181], час його виконання залежить від операндів, що є демаскуючим фактором. Цей алгоритм безпосередньо обчислює частку. Непрямий метод є експоненціальним (далі - Методи 2, 3 і 4 р. 3.4). Мультиплікативний зворотний елемент для β можна знайти ефективно у будь-якому базисі через $\beta^{-1} = \beta^k$, де k - будь-яке натуральне число, що задовольняє $k \equiv -1 (\mathrm{mod}\ m)$, де m - порядок β. Існує спеціалізований алгоритм [132] для експонування для $k = 2^m - 2$. Час його виконання не залежить від величини операндів, що є суттєвим для маскування роботи пристрою. Збільшення ефективності алгоритму є особливо суттєвим, коли піднесення до квадрату можна виконувати швидко (наприклад, у нормальному базисі).

У роботі [9] показано, що апаратне множення в поліноміальних та нормальних базисах вимагає приблизно рівних апаратних і часових витрати, але структурна складність помножувачів для нормального базису в m разів більша структурної складності помножувачів для поліноміального базису [45], [71], час програмного множення у поліноміальному базисі на 1-2 порядки менший, ніж час множення в нормальному базисі [9]. Але недоліком поліноміального базису і рекомендованого у [191] розширеного алгоритму Евкліда є залежність часу обчислення обернених елементів полів Галуа від значення операндів [9], що може демаскувати роботу пристрою.

Розвиток методу маскування операційних вузлів для полів Галуа, які

використовуються при КЗІ на основі ЕК полягає у вирівнюванні часу обчислення обернених елементів у поліноміальному базисі шляхом відмови від використання узагальненого алгоритму Евкліда на користь алгоритмів прямого двійкового ділення або експоненціальних алгоритмів. Використання експоненційних алгоритмів вимагає ефективного виконання операцій піднесення до квадрату або знаходження квадратного кореня. Тобто, метод передбачає введення до складу GF-процесора додаткових вузлів – квадратора і(або) вузла знаходження квадратного кореня. Маскування шляхом використання запропонованих методів призводить до збільшення часу знаходження оберненого елемента і (або) до збільшення апаратних витрат.

## 2.16. Висновки до розділу 2

**Другий** розділ присвячено вибору та обґрунтуванню напряму досліджень та проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, у розділі наведено методи вирішення поставлених задач, визначено загальну методику проведення досліджень.

У розділі запропоновано узагальнена модель операційних вузлів для полів Галуа, що використовуються при КЗІ на основі еліптичних кривих. На сучасному етапі, коли КЗІ впроваджуються у КФС, важливим стає забезпечення їх роботи у реальному масштабі часу. Це вимагає використання швидкодіючих апаратних рішень – спецпроцесорів, які реалізуються в програмовних логічних інтегральних схемах (ПЛІС). Як базу для проєктування засобів КЗІ взято багаторівневий спецпроцесора (СП), який при опрацюванні цифрових підписів виконує операції над точками еліптичних кривих.

Також визначено підходи до проєктування уточнених моделей операційних вузлів для полів Галуа, що використовуються при КЗІ на основі еліптичних кривих.

Проведено деталізацію вимог щодо захисту роботи засобів КЗІ, щодо роботи із електронним цифровим підписом, визначено загальну методику проведення дисертаційних досліджень та особливості реалізації засобів КЗІ на ПЛІС.

Основними операціями у розширених полях Галуа *GF(pm),* виконання яких вимагає найбільшого часу, є обчислення оберненого елемента та множення.

Операції над елементами розширених полів Галуа *GF(pm)* використовуються для виконання операцій над точками ЕК (додавання точок, подвоєння, множення на константу). Тому у розділі запропоновано метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$, який у цій роботі, в основному, базується на представленні помножувача для поліноміального базису як паралельного помножувача у вигляді набору модифікованих комірок Гілда і складається з методів оцінювання його часової, структурної та ємнісної складності.

Також у цьому розділі запропоновано метод оцінювання складності злому апаратних засобів КЗІ та вдосконалений метод вбудованого тестування операційних вузлів для полів Галуа, що використовуються при КЗІ на основі еліптичних кривих

# РОЗДІЛ 3
# СИНТЕЗ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

## 3.1. Апаратна реалізація алгоритмів роботи засобів КЗІ

Встановлені переваги апаратної реалізації на ПЛІС алгоритмів та багаторівневих ієрархічних структур, оцінка їхньої складності дозволяють уточнити багаторівневу структуру засобів КЗІ (рис. 2.3, таблиця 1.3) [11]. Уточнення полягає в розміщенні на нижньому рівні вузлів, що опрацьовують окремі розряди елементів полів Галуа, і мають для помножувачів вигляд модифікованих комірок Гілда. Кількість рівнів (таблиця 3.1) визначається алгоритмами роботи вузла відповідно до стандартів [93], [91], [90], [89]. Розподіл задач між різними рівнями також ілюструє таблиця 3.1.

*Таблиця 3.1*

**Розподіл задач між різними рівнями (ЕЦП відповідно до [93])**

| Рівень | Тип операцій | Операції |
|---|---|---|
| 4 (найвищий) | Основні перетворення | Отримання та перевіряння ЕЦП |
| 3 | Операції над точками ЕК | Додавання, подвоєння, множення на число |
| 2 | Операції над елементами поля Галуа | Множення, знаходження оберненого елемента, ділення, піднесення до квадрату, |
| 1 (найнижчий) | Операції над розрядами елементів поля Галуа і в модифікованих комірках Гілда | Додавання, пересилання, визначення розрядів добутку |

Структурну схему кожного рівня умовно можна поділити на протокольну та спеціалізовану частину (рис. 3.1). Протокольна частини містить двопортову пам’ять, «поштову скринька» для взаємодії з верхнім рівнем, універсальний процесор.

Універсальний процесор виконує протокольні функції, здійснює доступ до операційних пристроїв через свою локальну шину і забезпечує їхню роботу.

Спеціалізована частина є набором спецпроцесорів (рис. 3.2, СП, може складатися з одного СП).

Усі СП мають аналогічну структуру (рис. 3.3), яка відповідає рис. 3.1 та рис. 3.2.

Кожний СП складається з протокольної частини (на базі універсального процесора) і з спеціалізованої частини (СпП). Універсальний процесор (ПрП) при взаємодії з верхнім рівнем і своїм СпП виконує протокольні функції. Це дозволяє реалізувати універсальний процесор як процесор з скороченою СК (*RISC* [150]). У свою чергу СпП виконує обчислення у відповідності з переданими йому командою та даними під керуванням свого керуючого автомата (*FSM*).

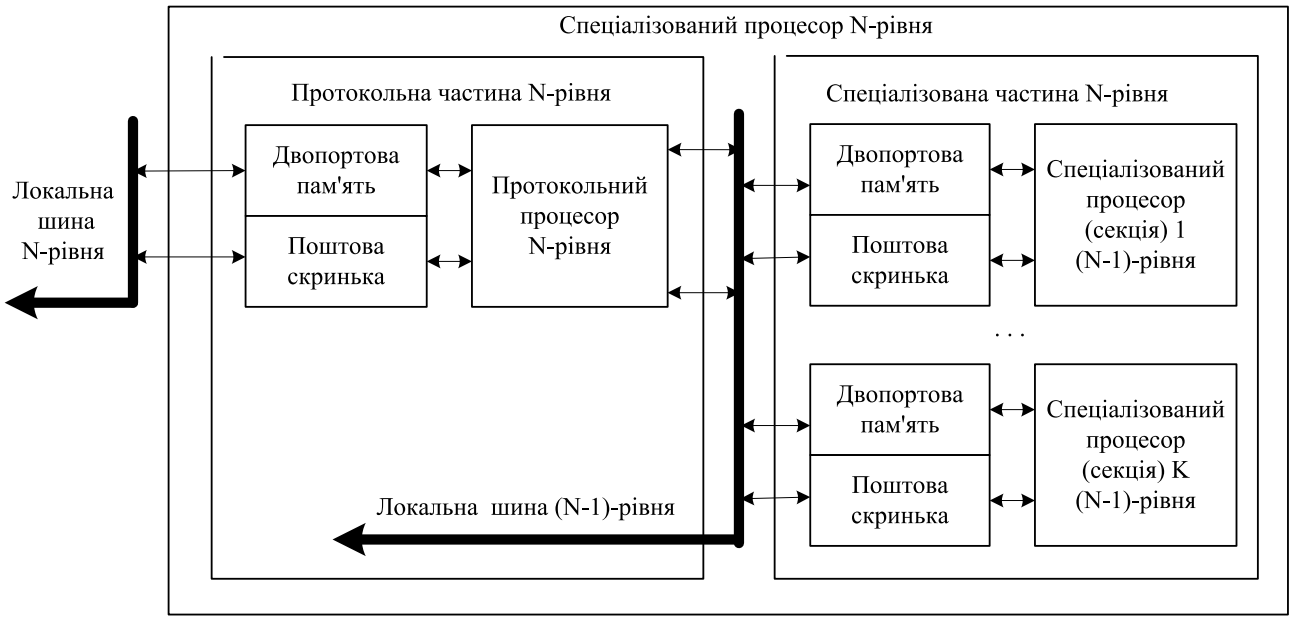



Рис. 3.1. Структура *N*-СП з декількома (*N*-1) СП

Протокольні процесори у цій дисертаційній роботі не розглядаються так само як і інтерфейс між ними та СпП.

Запропоновано модель одного із СП для опрацювання елементів полів Галуа (GF-процесор) показано на рис. 3.4 [151]. Його було обрано як основу для тестів згенерованих ядер. Даний спецпроцесор конфігуровано для поля GF($2^{163}$), а його операційний пристрій складається з помножувача MUL і арифметико-логічного блоку ALU. ALU виконує додавання та піднесення до квадрату. Необхідне для операцій над точками еліптичних кривих ділення може бути виконане програмним або мікропрограмним способом. Також GF-процесор має пристрій керування (контролер) і регістровий файл..

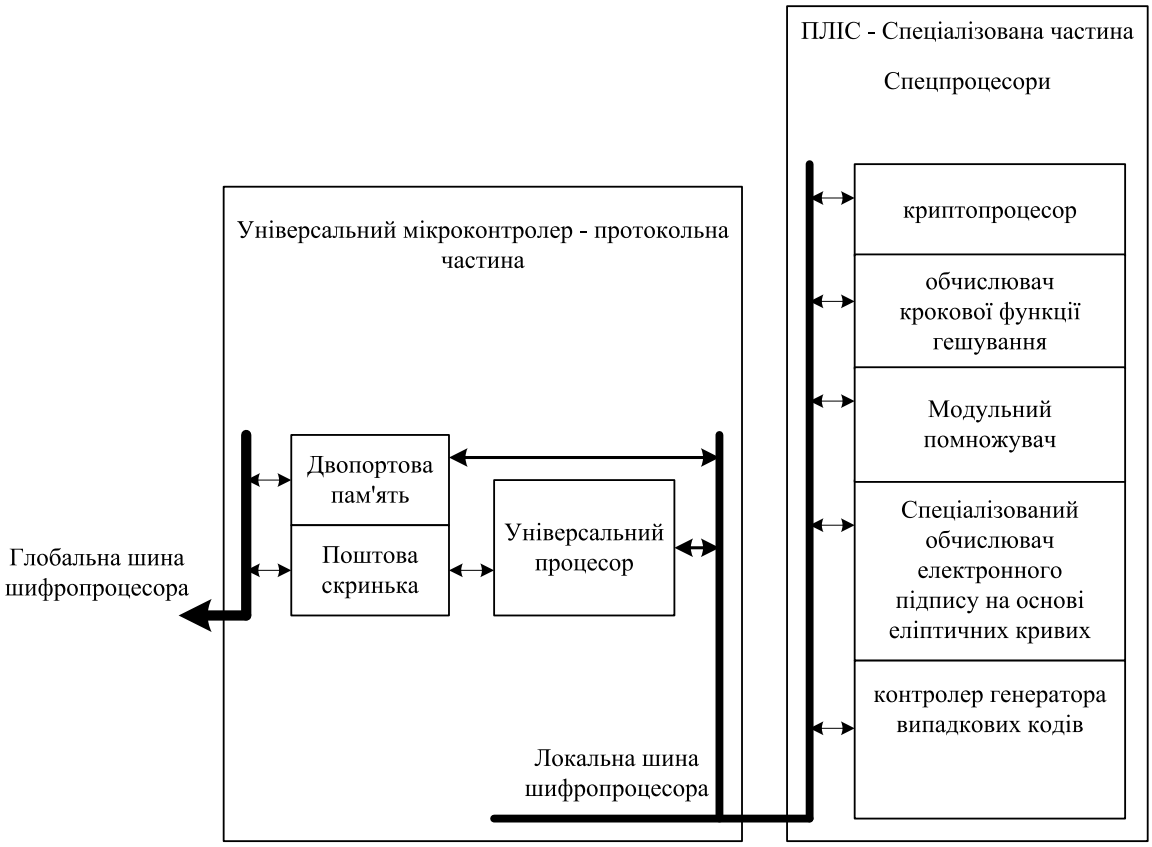



Рис. 3.2. Шифропроцесор

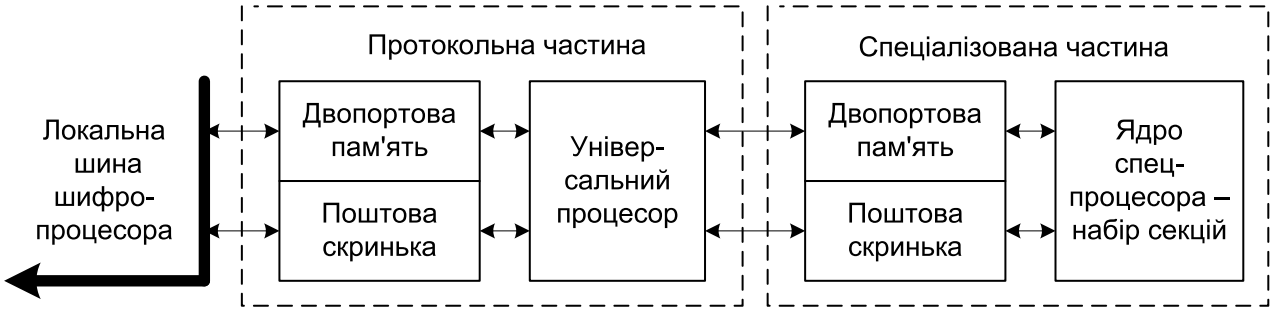



Рис. 3.3. Структура СП

## 3.2. Спецпроцесор для опрацювання елементів розширених полів Галуа

Модифіковану в рамках цього дослідження модель спецпроцесора (GF-процесора) показано на рис. 3.5. Компаратор було імплементовано лише для випробувань ядер, які реалізують алгоритми інверсії із змінним часом виконання.

Запропонований GF-процесор має додатковий функціональний блок для розміщення досліджуваних ядер (FumctionalUnit - FU на рис. 3.5), що відрізняє його від відомих рішень (рис. 3.4). Тому далі запропоновані варіанти ядер порівнювалися за величиною апаратних витрат на реалізацію функціонального блока FU. Частотні характеристики прототипу при цьому не досліджувалися.

Рис. 3.4. Спецпроцесор для двійкових полів Галуа

3.3. Технологічний засіб для проєктування операційних вузлів GF-процесора – генератор ядер

Для проведення досліджень у ході виконання роботи було розроблено технологічний засіб (генератор ядер) для проєктування помножувачів елементів полів Галуа $GF(p^m)$ для поліноміального базису, вузлів обчислення квадратних коренів, інверторів з незалежним від операндів часом обчислення .(рр.3.3.1, 3.4, 3.5). Генератор розроблено за методикою [62] з врахуванням досвіду [41], [42]. Генератор формує VHDL-описи вузлів знаходження обернених елементів (інверторів). Помножувачі опрацьовують $m$-бітні елементи полів Галуа $GF(p^m)$ і формують $m$-бітний добуток. Змінні $m$ та $p$ є параметрами, які користувач може задавати перед генерацією ядра.

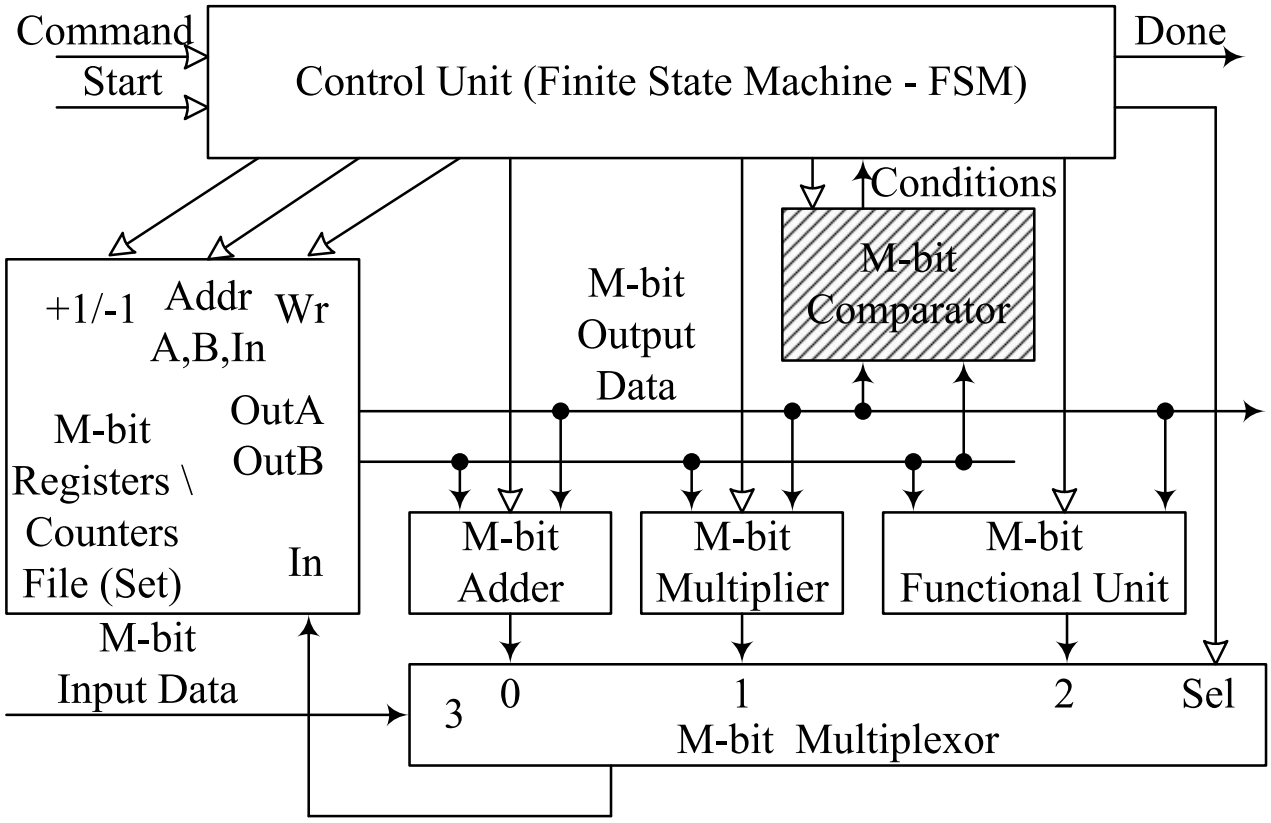



Рис. 3.5. GF-процесор з додатковим функціональним блоком

Основні параметри генератора, які може встановити користувач:

тип ядра;

метод створення ядра (інвертора - від 1 до 5);

характеристика p ($2 \le p \le 2^{1000}$) розширеного поля Галуа $GF(p^m)$;

степінь m ($3 \le m \le 1000$) розширеного поля Галуа $GF(p^m)$;

незвідний многочлен F, що утворює поле.

При цьому порядок поля $p^m$ не може перевищувати значення $2^{1000}$ ($p^m \le 2^{1000}$).

Основні етапи роботи генератора ядер: ввід параметрів $m$ та $p$; ввід утворюючого полінома поля $GF(p^m)$ для поліноміального базису; генерація помножувача.

Ядра інвертора генеруються як структуру стандартних логічних блоків:

SqrR – обчислювач квадратного кореня;

Sqr – square calculator (квадратор);

Mul – помножувач: біт-паралельний помножувач-акумулятор [158] або паралельний помножувач [153];

Rg – регістр;

MX - мультиплексор;

Cmp – компаратор (для випробувань ядер, які реалізують алгоритми інверсії із змінним часом виконання);

Cntr – вузол керування (цифровий автомат, FSM).

У моделі GF-процесора вже присутні деякі з цих блоків. Відсутні в моделі GF-процесора ядра схемотехнічно зібрано у додатковому функціональному вузлі (FU). Лише апаратні ресурси FU рахувалися в пп. 3.4, 3.5 як вартість обладнання для реалізації знаходження мультиплікативної інверсії (оберненого елемента).

Для дослідження всі частини кожного інвертора збираються в одному вузлі (ядрі). Схематичні символи описаних у п. 3.4 ядер представлено на рис. 3.6. Різниця між графічними символами ядер, сформованих методами 2-5, полягає лише в їхніх іменах.

Для досліджень було згенеровано ядра для GF($2^m$) з m = 64:

M: integer := 64;

logM: integer := 8;

F: std_logic_vector(M:0) := '1'& x"010100000101001B".

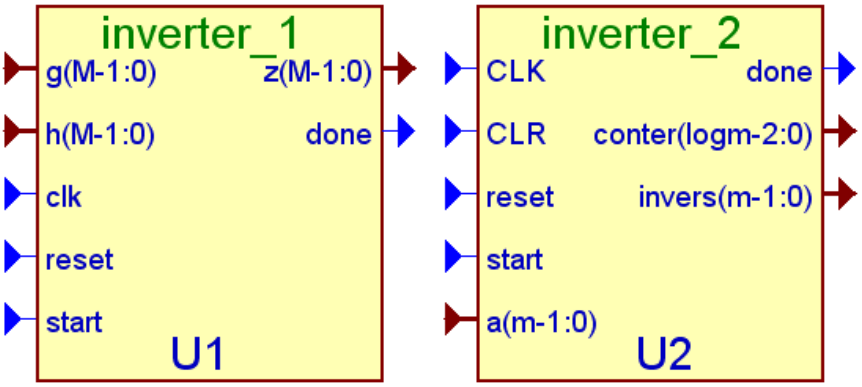



Рис. 3.6. Символи згенерованих ядер інверторів (U1 - метод 1, U2 – методи 2 - 5)

3.3.1. Ядра для обчислення квадратних коренів у двійкових полях Галуа

Необхідність маскування роботи операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК у поліноміальному базисі вимагає (для реалізації деяких з розглянутих алгоритмів) введення до складу процесора вузлів, що виконують обчислення квадратних коренів у двійкових полях Галуа. Огляд методів обчислення коренів у двійкових полях Галуа містить Додаток Л.

3.3.2. Реалізація обчислення квадратних коренів

Метод (Додаток Л) обчислення квадратного кореня використано при обчисленні обернених елементів у поліноміальному базисі (пп. 3.4.2, 3.5). Створене на його основі ядро використовує відомі вузли нижчого рівня суматор (Adder) та помножувач (Mult). У ядрі також використано ПЗП (ROM) та вузол розбиття на парні та непарні розряди (Half_even_odd). Його VHDL-опис містить Додаток М. Запропоновану модель вузла обчислення квадратного кореня (SRU) представлено на рис. 3.7.

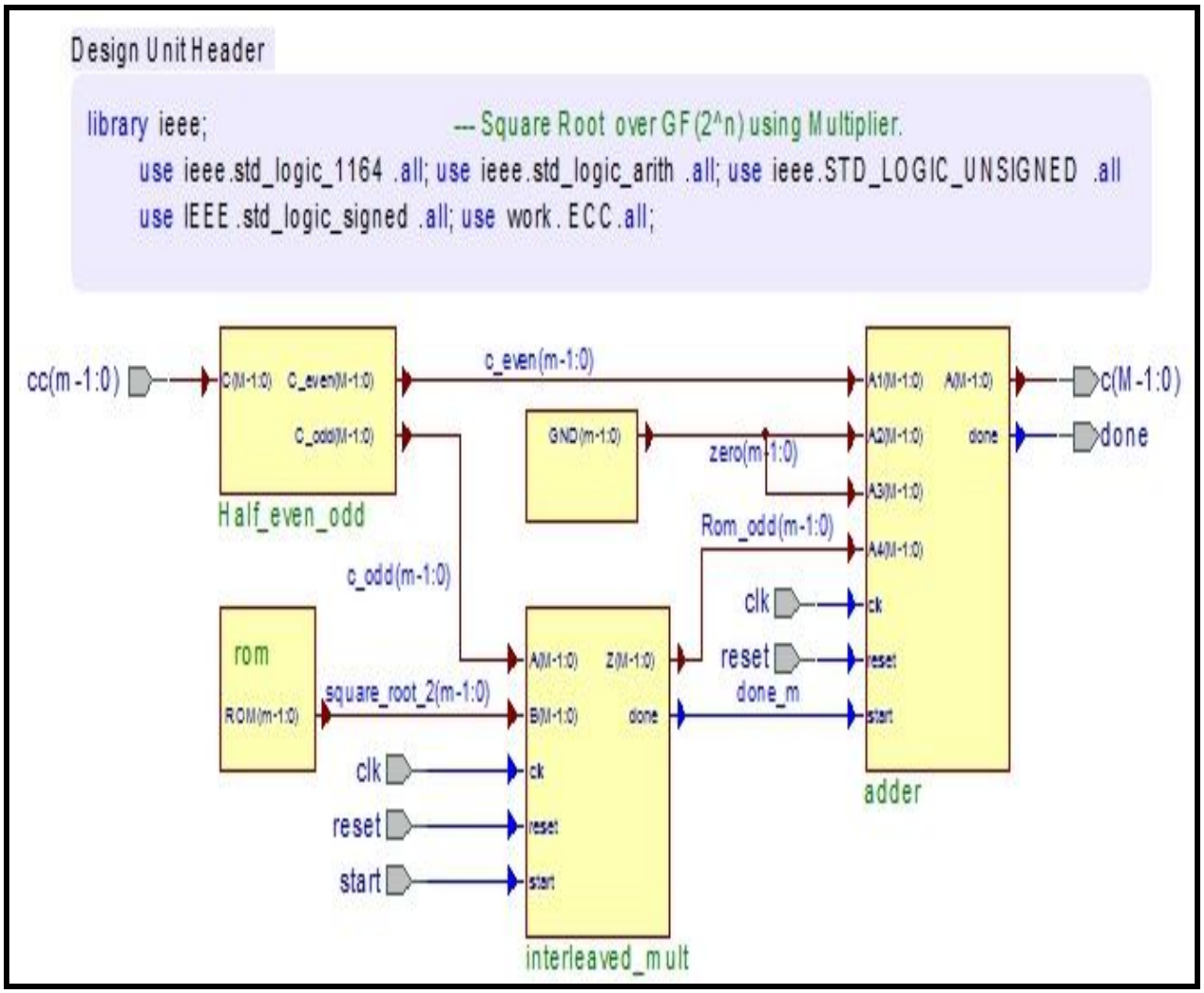



Рис. 3.7. Модель запропонованого вузла обчислення квадратного кореня

3.4. Маскування роботи інверторів на основі біт-паралельних помножувачів

Алгоритм інверсії з постійним часом виконання корисний проти класу атак сторонніми каналами. Реалізовані відповідно до запропонованих методів інвертування (р. 2.15) ядра інверторів з незалежним від операндів часом обчислення

досліджуються в поліноміальному базисі двійкових полів Галуа GF($2^m$) з метою вибору найкращого за апаратною та часовою складностями. Чотири з перевірених методів засновані на піднесенні до степеня, а один (Метод 1) є методом прямого ділення. Усі методи було реалізовано як ядра ПЛІС і було протестовано як частина спеціалізованого процесора для опрацювання елементів полів Галуа.

Біт-паралельна арифметика досить поширена [137] і базується на по-бітному аналізі одного з операндів з наступним виконанням якоїсь операції над усіма розрядами (паралельно) другого операнда.

Апаратні ресурси Xilinx xc6slx150tfgg900-3 [*202*] (кількість тригерів FF, комбінаційних елементів LUT і слайсів) для всіх методів реалізації інверторів представлено в Таблиці 3.2, де також містяться відомості про період синхроімпульсів та їхню кількість, необхідну для обчислення для мультиплікативної інверсії.

3.4.1. Метод прямого апаратного ділення

Згідно з цим методом GF-процесор з помножувачем повинен мати додатковий дільник - функціональний блок (FU) на рис. 3.5. Незалежний від значень операндів алгоритм взято з [118].

Алгоритм двійкового ділення: *z(x)=g(x)/h(x) mod f(x)*.

**Input:** a(x):=f(x);b(x):=h(x);u(x):=0;v(x):=(g(x) or 1); **output**: z(x).

1. $\alpha := m;\ \beta := m-1$
2. *while* $\beta \geq 0$ *loop*

*if* $b_0 = 0$ *then* $b(x) := b(x)/x;\ v(x) := v(x).x^{-1} \bmod f(x);$

$\beta := \beta - 1;$

*else*

$b(x) := (a(x)+b(x))/x;$

$v(x) := (u(x)+v(x)) \cdot x^{-1} \bmod f(x);$

*if* $\alpha > \beta$ *then*

$a(x) := b(x);\ u(x) := v(x);$

$(\alpha,\beta) := (\beta,\alpha-1);$

*else*

$\beta := \beta - 1;$

*end if;*

*end if;*

3. *end loop;*

4. $z(x) := u(x);$

Для мультиплікативної інверсії можна використовувати цей алгоритм, якщо прийняти $v(x)=1$, де $h(x)^{-1} = 1 \cdot h(x)^{-1} \bmod f(x)$.

Всі апаратні ресурси для методу 1 є частиною FU.

*Таблиця 3.2*

**Технічні ресурси функціонального блоку FU**

| Method (m=64) | 1 | 2 | 3 | 4, 5 |
|---|---|---|---|---|
| # Slices, total (S) | 111 | 289 | 119 | 139 |
| Total # FFs | 278 | 902 | 556 | 353 |
| Total # LUTs | 333 | 981 | 498 | 447 |
| # FFs in FU | 278 | 406 | 203 | 0 |
| # LUTs in FU | 333 | 598 | 246 | 201 |
| Min clock period (P, ns) | 4.053 | 4.174 | 3.305 | 3.263 |
| # clocks (C) | 131 | 2374 | 8629 | 4535 |
| Комплексний показник (CI =S*P*C/$10^6$) | 0,06 | 2,86 | 3,39 | 2,06 |

3.4.2. Мікропрограмні методи ділення

3.4.2.1. Метод 2 (обчислення квадратного кореня та піднесення до квадрату)

Оскільки мультиплікативна група поля Галуа GF($2^n$) є циклічною з порядком $2^n$-1 для будь-якого ненульового елемента $a \in GF(2^n)$, обернений елемент $a^{-1}$ у полі $GF(2^n)$ можна обчислити, використовуючи метод [132] наступним чином: за теоремою Лагранжа, $a^{2^m-1} = 1$, це означає, що $a^{2^m-2} = a^{-1}$. Для ефективного виконання такого піднесення до степеня використовується наступний ланцюжок додавання: $a^{2^m-2} = (a^{2^{m-1}-1})^2$. Зрозуміло, що $2^m - 2 = 2(2^{m-1} - 1) = 2\sum_{j=0}^{m-2} 2^j = \sum_{j=1}^{m-1} 2^j$.

Найбільш правий компонент згаданих вище рівнянь дозволяє нам виразити мультиплікативний обернений елемент в такий спосіб: $(a^{2^{m-1}-1})^2 = a^{-1} = \prod_{j=1}^{m-1} a^{2^j}$. Для будь-якого ненульового $a \in GF(2^m)$, ми маємо $a^{2^{-1}} = a^{2^{m-1}}$ і $\forall j \le m-1$; $a^{2^{-j}} = a^{2^{m-j}}$, тоді ми

отримаємо $a^{-1} = \prod_{j=m-1}^{1} a^{2^{m-j}} = \prod_{j=m-1}^{1} a^{2^{-j}} = a^{\sum_{j=m-1}^{1} 2^{-j}}$ (зауважте, що всі індекси змінюються в порядку зменшення). Відмічаємо

$$\sum_{j=m-1}^{1} 2^{-j} = \frac{1-\left(\frac{1}{2}\right)^m}{1-\left(\frac{1}{2}\right)} - 1 = \frac{2^m - 1}{2^{m-1}} - 1 =$$

$$= \sum_{j=m-1}^{1} 2^{-j} = \frac{2^{m-1} - 1}{2^{m-1}} \Rightarrow a^{-1} = a^{\frac{2^{m-1}-1}{2^{m-1}}}.$$

Запропонований алгоритм обертає елемент з використанням квадратного кореня та піднесення до квадрату у поліноміальному базисі з розрахунковим часом, незалежним від коду елемента x наступним чином:

$$a^{-1} = \left(a^{2^{\pm\left(\frac{m}{2}\right)}}\right)^{E\_O} \otimes \prod_{j=1}^{\frac{m-1-E\_O}{2}} a^{2^j} \otimes a^{2^{-j}} \qquad (1)$$

$$a^{-1} = \left(a^{2^{\pm\left(\frac{m}{2}\right)}}\right)^{E\_O} \otimes \prod_{j=1}^{\frac{m-1-E\_O}{2}} a^{2^j} \otimes \prod_{j=1}^{\frac{m-1-E\_O}{2}} a^{2^{-j}} \quad (2)$$

Де E_O = Even_odd = (m-1)mod 2.

Алгоритм 2 методу:

**Input**: $a \in GF(2^m)$ *for* $m \geq 3$;

E_O =(m-1)mod 2.

Output: $A^{-1}$

1. *Beta ← (m-1-E_O)/2; P← 1;*
   $R = \sqrt{A}$ ; $S = A^2$.
2. *Compute* $P_{RS} = R \times S$.
3. *Compute* $P = P \times P_{RS}$; *Beta=Beta-1.*
4. *If Beta = 0 then go to last step 5.*
   *Else* $R = \sqrt{R}$ ; $S = S^2$.
   *Go to step 2.*
5. *If (E_O = 0) then* $A^{-1} = P$
   *Else* $A^{-1} = P \times \sqrt{R}$ *or* $A^{-1} = P \times S^2$.
   *Return* $A^{-1}$.

Детальний список апаратних ресурсів для методу 2 показано в Таблиці 3.3.

Лише частина апаратних ресурсів за методом 2 розміщується в FU.

*Таблиця 3.3*

**Детальний список ресурсів для методу 2**

| By Hierarchy | # FFs | # LUTs | Placed in |
|---|---|---|---|
| **Method 2 (m=64):** | 902 | 981 | |
| **Sqr** | 0 | 150 | FU |
| **SqrR** | 203 | 241 | FU |
| **Mul1** | 203 | 272 | |
| **Mul2** | 203 | 207 | FU |
| **Rg1** | 64 | 0 | |
| **Rg2** | 64 | 0 | |
| **Rg3** | 128 | 0 | |
| **Mx1** | 0 | 8 | |
| **Mx2** | 0 | 37 | |
| **Cmp** | 0 | 22 | |
| **Cntr** | 7 | 4 | |

3.4.2.2. Метод 3 (обчислення квадратного кореня і множення)

У цьому методі також використовується обчислення квадратного кореня для знаходження оберненого елемента у поліноміальному базисі. Алгоритм схожий на метод дотичних Ньютона-Рафсона [104]. Але інвертор має додаткову внутрішню затримку, щоб гарантувати той самий час розрахунку для будь-якого аргументу часу:

1. $P_0 = \sqrt{A}$ - Це початкове значення для і у циклі від 0 до *M*-2;
2. $P_i = \sqrt{A} \times P_{i-1}$;
3. *If* $P_i$*=1 then go to (4)*
   *Else go to (2)*;
4. $A^{-1} = P_{i-1}$.

Приклад обчислення містить Додаток К.

Детальний список апаратних ресурсів для методу 3 показано в Таблиці 3.4. Лише частина апаратних ресурсів за методом 3 розміщується в FU.

*Таблиця 3.4*

**Детальний список ресурсів для методу 3**

| By Hierarchy | # FFs | # LUTs | Placed in |
|---|---|---|---|
| **Method 3 (m=64):** | 556 | 498 | |
| **Mul** | 203 | 208 | |
| **SqrR** | 203 | 246 | FU |

| | | | |
|---|---|---|---|
| **Rg1** | 64 | 0 | |
| **Cntr** | 7 | 2 | |
| **Rg2** | 64 | 0 | |

3.4.2.3. Метод 4 (піднесення до квадрату і множення)

Тут квадрат використовується так само, як у методі 3:

1. $P_0 = a$; it is initial value for $i$ in 0 to $M$-2 loop;
2. $P_i = a \times P_{i-1}^2$;
3. *If* $P_i$*=1 then go to (4)*
   *Else go to (2);*
4. $A^{-1} = P_{i-1}^2$.

Детальний список апаратних ресурсів для методу 4 показано в Таблиці 3.5. Лише частина апаратних ресурсів за методом 4 розміщується в FU.

*Таблиця 3.5*

**Детальний список ресурсів для методів 4 та 5**

| **By Hierarchy** | **# FFs** | **# LUTs** | **Placed in** |
|---|---|---|---|
| **Method 4, 5 (m=64):** | 353 | 447 | |
| **Sqr** | 0 | 201 | FU |
| **Rg1** | 64 | 0 | |
| **Rg2** | 64 | 0 | |
| **Mul** | 203 | 205 | |
| **Cntr** | 7 | 8 | |
| **Mx** | 0 | 20 | |

3.4.2.4. Метод 5 (піднесення до квадрату і множення)

Тут квадрат також використовується для обчислення оберненого елемента у поліноміальному базисі. Використовується алгоритм [132]. Ресурси подібні до методу 4.

3.4.3. Висновок

Дослідження показали, що можна вирішити проблему знаходження оберненого елемента у двійкових полях Галуа у поліноміальному базисі за часом, незалежним від операндів.

Дослідження показали, що всі п'ять розглянутих методів дозволяють синтезувати ядра інверторів, які здатні знаходити обернений елемент у двійкових полях Галуа у поліноміальному базисі за часом, незалежним від значення операндів. Результати імплементацій ядер наведено в цьому розділі. Три методи може бути рекомендовано для використання. Метод 1 (метод прямого апаратного ділення)

забезпечує мінімальний час для пошуку оберненого елемента. Методи 4 та 5 вимагають найменшої кількості апаратних витрат (в півтора рази менше, ніж метод 1), але збільшують час знаходження оберненого елемента більш ніж у 30 разів у порівнянні з методом 1.

## 3.5. Маскування роботи інверторів на основі паралельних помножувачів

### 3.5.1. Ядра функціональних вузлів GF-процесора

Схематичні символи згенерованих за допомогою генератора (р. 3.3.1) ядер показано на рис. 3.8, де інвертор U1 використовує тільки помножувач, U2 використовує помножувач і квадратор, U3 використовує помножувач, квадратор і вузол обчислення квадратного кореня (метод 2 в р. 3.4.2.1).

Для ядер з $m$=64 було згенеровано такі параметри:

M: integer := 64; logM: integer := 8;

F: std_logic_vector(M:0) := '1'& x"010100000101001B".

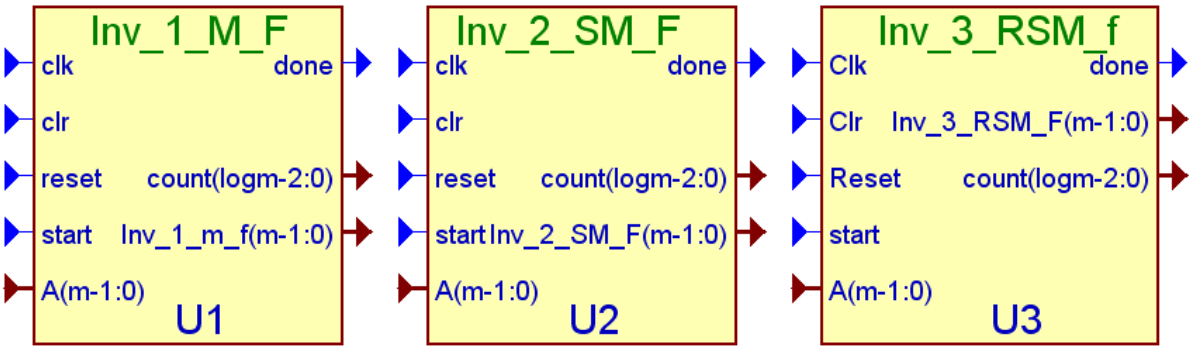



Рис. 3.8. Схемотехнічні символи згенерованих ядер з швидкими помножувачами

### 3.5.2. Мікропрограмні методи ділення

#### 3.5.2.1. Метод SRS (обчислення квадратного кореня та піднесення до квадрату)

Метод аналогічний методу, викладеному у р. 3.4.2.1.

Загальні ресурси апаратного забезпечення (кількість тригерів, комбінаційних схем (LUT) та слайсів) для методу SRS показано в Таблиці 3.6, де також містяться відомості про період синхроімпульсів та їхню кількість, необхідну для обчислення мультиплікативного оберненого елемента. Також наведено комплексний показник CI, кращий метод має найнижче значення цього показника.

Детальний список апаратних ресурсів для методу SRS показано в Таблиці 3.7.

Лише частина апаратних ресурсів за методом SRS розміщується в FU.

3.5.2.2. Метод SM (піднесення до квадрату і множення)

Тут піднесення до квадрату також використовується для обчислення оберненого елемента у поліноміальному базисі. Використовується алгоритм [132]. Метод аналогічний методу р. 3.4.2.4.

*Таблиця 3.6*

**Список ресурсів для інверторів з швидкими помножувачами (m = 64)**

| Method | SRS | SM | M |
|---|---|---|---|
| Total # Slices (S) | 919 | 792 | 699 |
| Total # FFs | 277 | 82 | 78 |
| Total # LUTs | 2934 | 2523 | 2334 |
| # FFs in FU | 0 | 0 | 0 |
| # LUTs in FU (L) | 514 | 476 | 0 |
| Min clock period (P, ns) | 9.8 | 10.0 | 9.4 |
| # clocks (C) | 126 | 126 | 250 |
| complex indicator (CI =S*P*C/$10^6$) | 1,13 | 1,00<br>1,13 | 1,64<br>1,00 |

1,64

*Таблиця 3.7*

**Детальний список ресурсів для методу SRS , m=64**

| By Hierarchy | # FFs | # LUTs | Placed in |
|---|---|---|---|
| SRS Method | 277 | 2934 | |
| Sqr | 0 | 127 | FU |
| SqrR | 0 | 414 | FU |
| Mul | 0 | 2168 | |
| MX_1 | 0 | 65 | |
| MX_2 | 0 | 65 | |
| MX_3 | 0 | 68 | |
| MX_4 | 0 | 70 | |
| Rg | 256 | 0 | |
| Cntr | 7 | 9 | |

Перевірену функціональну схему інвертора, у якому було реалізовано метод SRS, показано на рис. 3.9.

Загальні ресурси апаратного забезпечення (кількість тригерів, комбінаційних схем (LUT) та слайсів) для методу SM показано в Таблиці 3.6.

Детальний список апаратних ресурсів для методу SM показано в Таблиці 3.8. Лише частина апаратних ресурсів за методом SM розміщується в FU.

Перевірену функціональну схему інвертора, у якому було реалізовано метод SM, показано на рис. 3.10.

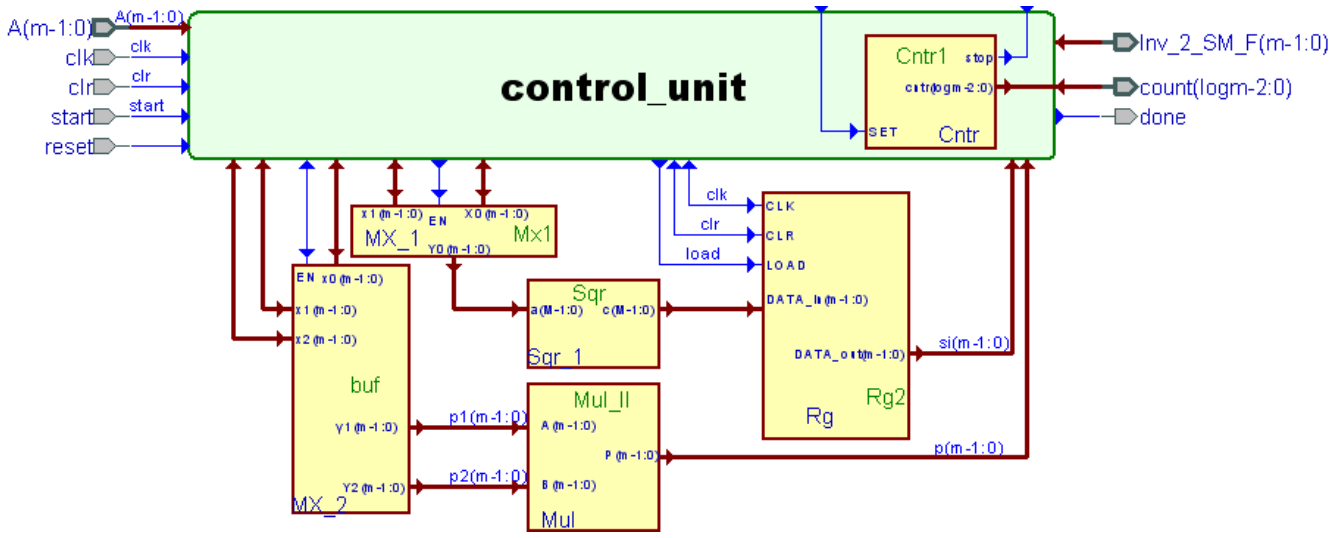



Рис. 3.9. Інвертор, який реалізує метод SRS

*Таблиця 3.8*

**Детальний список ресурсів для методу SM , m=64**

| By Hierarchy | # FFs | # LUTs | Placed in |
|---|---|---|---|
| SM Method | 82 | 2523 | |
| Sqr | 0 | 476 | FU |
| Mul | 0 | 1167 | |
| MX_1 | 0 | 782 | |
| MX_2 | 0 | 83 | |
| Rg | 64 | 0 | |
| Cntr | 7 | 8 | |

3.5.2.3. Метод M, заснований лише на використанні множення

Тут піднесення до квадрату також використовується для обчислення оберненого елемента у поліноміальному базисі, але виконується ця операція на помножувачі, тому ніякі додаткові елементи (FU) не входять до складу процесора GF (рис. 3.5).

Загальні ресурси апаратного забезпечення (кількість тригерів, комбінаційних схем (LUT) та слайсів) для методу M показано в Таблиці 3.6.

Детальний список апаратних ресурсів для методу M показано в Таблиці 3.9. Жодних апаратних ресурсів за методом M немає у FU.

Дослідження показали, що всі розглянуті методи, що базуються на використанні обчислень квадратів та квадратних коренів та використанні швидких паралельних помножувачів у спеціалізованому GF-процесорі, дозволяють синтезувати ядра інверторів, які здатні знаходити обернені елементи у двійкових полях Галуа на поліноміальній основі за часом, незалежним від значення операндів.

Результати імплементацій ядер наведено в цьому розділі. Метод на основі алгоритму [132] (піднесення до квадрату та множення) можна рекомендувати також і для використання з поліноміальним базисом. Він забезпечує мінімальні часові витрати для обчислення оберненого елемента, для цього потрібні менші апаратні витрати в порівнянні з методи, заснованими на обчисленні квадратних коренів та квадратів.

*Таблиця 3.9*

**Детальний список ресурсів для методу M , m=64**

| By Hierarchy | # FFs | # LUTs | Placed in |
|---|---|---|---|
| M Method | 78 | 2334 | |
| Mul | 0 | 2178 | |
| MX | 0 | 138 | |
| Rg | 64 | 0 | |
| Cntr | 7 | 10 | |

Перевірену функціональну схему інвертора, у якому було реалізовано метод SM, показано на рис. 3.11.

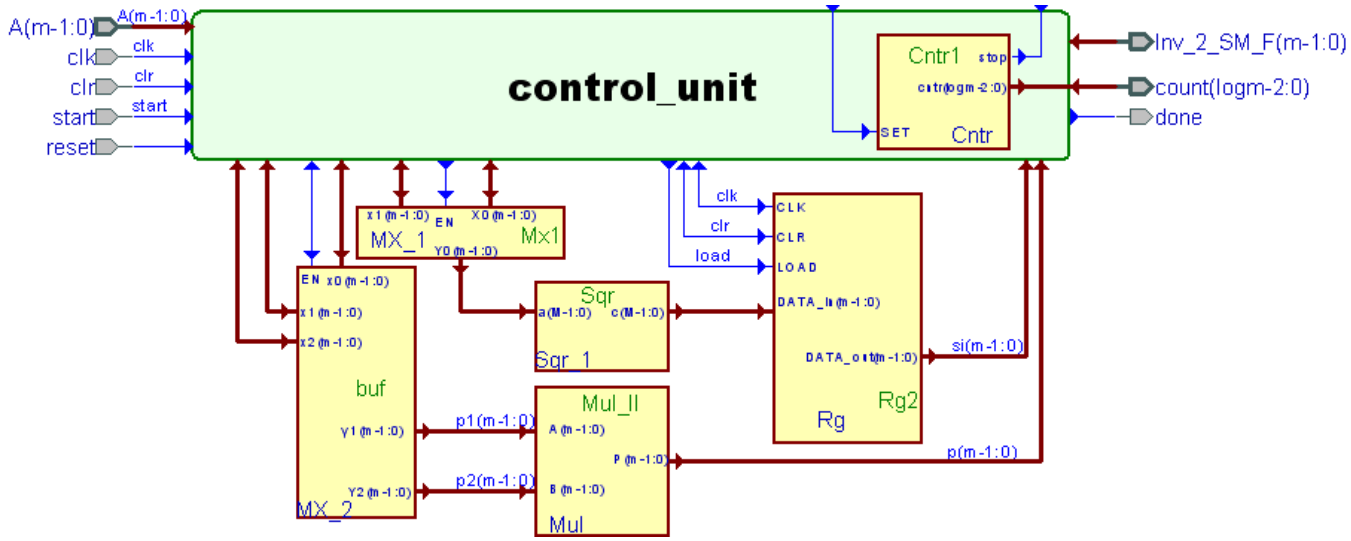



Рис. 3.10. Інвертор, який реалізує метод SM

## 3.6. Рекомендована послідовність проєктування уточнених структурних моделей операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК

Проєктування уточнених структурних моделей операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК базується на методі проєктування багаторівневих комп'ютерних систем [11], [12] і складається з послідовності проєктних рішень (аналіз / реалізація):

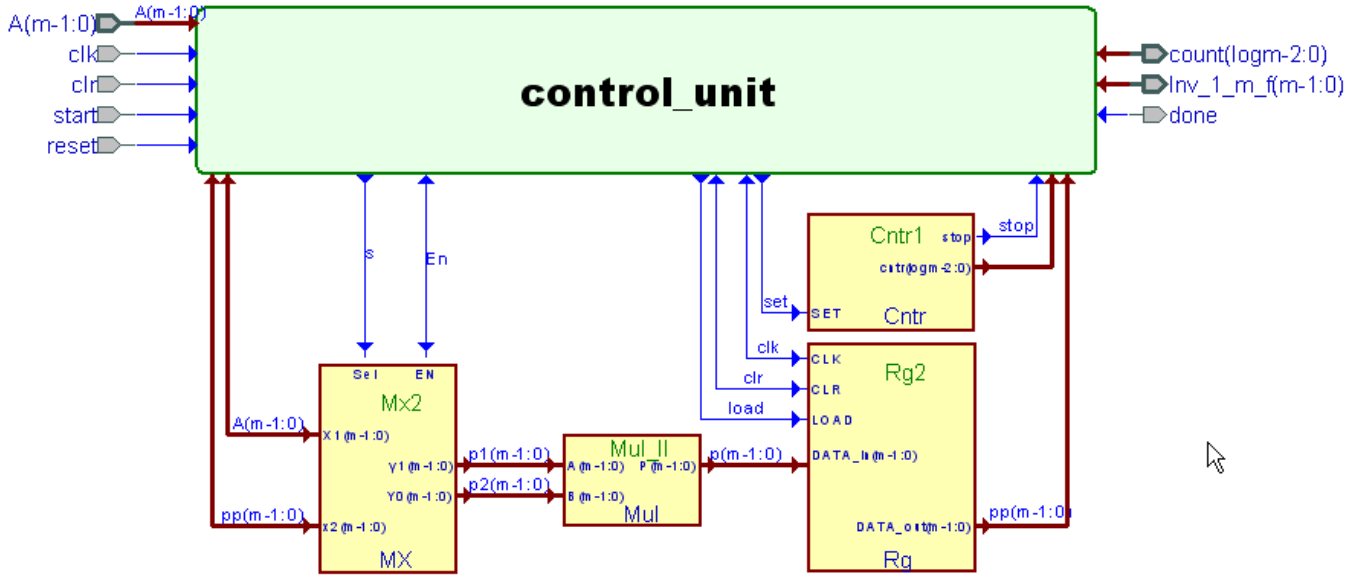



Рис. 3.11. Інвертор, який реалізує метод М

елементна база обирається з врахуванням сучасних технологічних рішень – ПЛІС, ядер (р. 1.9 / р. 3.1);

система представляється як багаторівнева структура відповідно до еталонної моделі взаємозв'язку відкритих систем (р. 1.8 / р. 3.1);

кількість рівнів N визначається обраними алгоритмами (р. 1.8);

для несекційних операційних пристроїв кожний *N*-рівень є *N*-СП, який складається з ПрП *N*-рівня і декількох СП (*N*-1)-рівня (р. 1.8 );

кожний ПрП *N*-рівня реалізується як універсальний процесор (р. 1.8);

кожний із СП реалізує одне або декілька із покладених на нього завдань (рр. 1.8, 1.8.3);

кожний із СП працює відповідно до обраного стандарту (Розділ 3);

кількість СП визначається потоком даних та заданим часом їхнього опрацювання (р. 1.8);

операційні пристрої реалізуються у вигляді ядер НВІС (практично – ПЛІС) (р. 1.9);

ядра проєктуються з врахуванням необхідності маскування роботи КЗ (р. 1.13);

ядра проєктуються з засобами вбудованого контролю (р. 2.14);

процес проєктування ядер розділяється на чотири нитки визначених у р. 1.10: (1) програмування ПрП, (2) проєктування апаратного забезпечення СП, (3)

проєктування технологічних засобів для моделювання та перевіряння роботи спроєктованих вузлів і (4) проєктування технологічних засобів для перевіряння засобів вбудованого контролю (р. 1.10);

Даний підхід дозволяє створити модульну ієрархічну структуру, до якої застосовуються методи паралельного і одночасного проєктування, виготовлення, налагодження і тестування.

## 3.7. Висновки до розділу 3

У третьому розділі уточнено багаторівневу ієрархічну структуру апаратної реалізації алгоритмів роботи засобів КЗІ. Уточнення полягає в розміщенні на нижньому рівні вузлів, що опрацьовують окремі розряди елементів полів Галуа, і мають для помножувачів вигляд модифікованих комірок Гілда.

Структурну схему кожного рівня умовно можна поділити на протокольну та спеціалізовану частину (рис. 3.1). Протокольна частини містить двопортову пам’ять, «поштову скринька» для взаємодії з верхнім рівнем, універсальний процесор.

Універсальний процесор виконує протокольні функції, здійснює доступ до операційних пристроїв через свою локальну шину і забезпечує їхню роботу.

Спеціалізована частина є набором спецпроцесорів (рис. 3.2, СП, може складатися з одного СП).

Усі СП мають аналогічну структуру.

У розділі представлено спецпроцесор для опрацювання елементів розширених полів Галуа – GF-процесор, його операційний пристрій складається з помножувача MUL і арифметико-логічного блоку ALU. ALU виконує додавання та піднесення до квадрату. Необхідне для операцій над точками еліптичних кривих ділення може бути виконане програмним або мікропрограмним способом. Також GF-процесор має пристрій керування (контролер) і регістровий файл.. Запропонований GF-процесор має додатковий функціональний блок для розміщення досліджуваних ядер, що відрізняє його від відомих рішень.

Для проведення досліджень у ході виконання роботи було розроблено технологічний засіб (генератор ядер) для проєктування помножувачів елементів полів Галуа *GF(pm)* для поліноміального базису, вузлів обчислення квадратних

коренів, інверторів з незалежним від операндів часом обчислення.

Основні параметри генератора, які може встановити користувач:

тип ядра;

метод створення ядра (інвертора - від 1 до 5);

характеристика p ($2 \le p \le 21000$) розширеного поля Галуа *GF(pm)*;

степінь m ($3 \le m \le 1000$) розширеного поля Галуа *GF(pm)*;

незвідний многочлен F, що утворює поле.

При цьому порядок поля *pm* не може перевищувати значення 21000 ($pm \le 21000$).

У розділі запропоновано метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі, який полягає у вирівнюванні часу обчислення обернених елементів у поліноміальному базисі шляхом відмови від використання узагальненого алгоритму Евкліда на користь алгоритмів прямого двійкового ділення або експоненціальних алгоритмів. Використання експоненційних алгоритмів вимагає ефективного виконання операцій піднесення до квадрату або знаходження квадратного кореня. Тобто, метод передбачає введення до складу GF-процесора додаткових вузлів – квадратора і(або) вузла знаходження квадратного кореня. Маскування шляхом використання запропонованих методів призводить до збільшення часу знаходження оберненого елемента і (або) до збільшення апаратних витрат.

Необхідність маскування роботи операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК у поліноміальному базисі вимагає (для реалізації деяких з розглянутих алгоритмів) введення до складу процесора вузлів, що виконують обчислення квадратних коренів у двійкових полях Галуа. У розділі проведено дослідження методів обчислення коренів у двійкових полях Галуа і реалізованих з їх використанням ядер для GF-процесора.

У розділі порівняно маскування роботи інверторів на основі біт-паралельних та паралельних помножувачів, визначено методи, які забезпечують найменші апаратні витрати, і методи, які найменше збільшують час обчислень оберненого

елемента. Результати дослідження викладено у вигляді таблиць і проілюстровано схемами запропонованих ядер.

Усі розглянуті методи інвертування дозволяють синтезувати ядра інверторів, які здатні знаходити обернені елементи у двійкових полях Галуа на поліноміальній основі за часом, незалежним від значення операндів.

Необхідні для інвертування додаткові елементи GF-процесора займають від 119 до 919 слайсів і забезпечують час інвертування від 131 до 8629 нс (GF(264)), що дозволяє обирати ядра в залежності від потреб замовника.

Результати проєктування інверторів для GF-процесора узагальнено у вигляді рекомендованої послідовності проєктування уточнених структурних моделей операційних вузлів для полів Галуа, що використовуються при КЗІ на основі еліптичних кривих.

Даний підхід дозволяє створити модульну ієрархічну структуру засобів КЗІ та розпаралелити роботи на етапах проєктування, виготовлення, налагодження і тестування.

# РОЗДІЛ 4
# ДОСЛІДЖЕННЯ ТА ВПРОВАДЖЕННЯ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

## 4.1. Впровадження результатів дисертаційної роботи

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом) (Додаток А, Додаток Б).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»), що підтверджено відповідним Актом (Додаток В).

## 4.2. Розробка та дослідження уточнених структурних моделей операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК і впровадження результатів у ДБ «Кібер»

Характеристики комп'ютера, на якому було отримано більшість кількісних параметрів досліджуваних вузлів викладено нижче [198].

Name, producer: Aser Aspire 4830TG - 2012.

CPU : Intel inside TM core TM i5.

frequency: 2.9 GH.

memory: 4 GB.

Windows 10 , 64 bit

4.2.1. **Мета та задачі проєкту Кібер.**

Метою держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446) було розроблення методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі КФС, теоретичних основ побудови КФС та принципів їх функціонування і практичної реалізації у вигляді масштабованої, гнучкої, реконфігуровної та нарощуваної базової платформи, у складі якої організується захищена взаємодія вимірювально-обчислювальних, керуючих, комунікаційних та виконавчих компонентів.

Серед завдань, на вирішення яких було спрямовано проєкт Кібер, і до виконання яких було залучено автора цієї роботи, було, у тому числі, дослідження та розроблення принципів захищеного обміну, опрацювання та зберігання вимірювальної та службової інформації, в тому числі способів забезпечення конфіденційності, цілісності та автентичності інформації, технічного та криптографічного захисту інформаційних зв’язків між компонентами КФС та управління доступом до них, розроблення методологічних засад інформаційної та функціональної безпеки **[**103**]**.

Отримані в ході виконання ДБ/КІБЕР результати знайшли своє відображення в монографії [76].

4.2.2. Ядро ПЛІС операційного вузла для полів Галуа, які використовуються для цифрового підпису на основі еліптичних кривих

При проведенні ДБ «Кібер» для розроблення та дослідження нових принципів захищеного обміну інформацією та організації в рамках відкритої апаратно-програмної платформи КФС з орієнтацією на полія Галуа, використання яких є першочерговою задачею і регламентується діючими стандартами (п. 1.6.5), автором було розроблено набір програмних засобів, які дозволяють міняти деякі параметри моделей вузлів – генератор ядер (п. 3.3) , а з його допомогою - набір ядер ПЛІС (моделі) операційних вузлів для опрацювання елементів розширених двійкових

полів Галуа та точок еліптичних кривих, які використовуються при виконанні алгоритмів роботи із цифровими підписами [154], [153], [159]. Об'єднання цих ядер утворює у ПЛІС так званий процесор еліптичних кривих. Первинно ці ядра було створено для роботи в двійкових розширених полях $GF(2^m)$ у поліноміальному базисі, у ході роботи їх було модифіковано для роботи у полях $GF(p^m)$ з характеристиками $p > 2$. У ході роботи частина моделі процесора еліптичних кривих – його арифметичний блок AU та контролер арифметичного блоку AUC було вдосконалено до так званого GF-процесора (рис. 3.5), який використовувався у подальшій роботі як стенд для перевірки висунутих теоретичних положень і їх порівняння з практичними результатами імплементації ядер у ПЛІС.

Модель реалізованого в ході роботи на ПЛІС процесора еліптичних кривих, відповідає багаторівневій структурі функціонального каналу (рис. 2.1, рис. 2.16) і представлена на рис. 4.1. На рис. 4.1 процесор еліптичних кривих складається з арифметичного пристрою та двох програмованих процесорів - головного контролера та контролера арифметичного пристрою. Головний контролер (MC, рис. 4.2). ) та контролер арифметичного вузла (AUC, рис. 4.3) - це процесори з архітектурою RISC MC відповідає за керування процесом множення точки еліптичної кривої.

AUC відповідає за обробку команд MC. AUC обробляє команди MC, керуючи AC шляхом визначення необхідних арифметичних операцій. При виконанні множення точок AUC несе відповідальність за виконання на AC операцій додавання та віднімання точок, подвоєння точок,координатних перетворень, множення та інверсії у полі.

Арифметичний блок (AU, рис. 4.4) є основним вузлом процесора еліптичної кривої. Продуктивність AU визначає продуктивність процесора еліптичної кривої. Для високопродуктивних процесорів еліптичних кривих, складність AC також визначає складність процесора еліптичних кривих, оскільки для цих реалізацій сукупна складність MC і AUC є низькою в порівнянні зі складністю AC.

AC несе відповідальність за доповнення, віднімання, множення, інверсію та порівняння елементів полів Галуа. AC також несе відповідальність за зберігання параметрів еліптичних кривих, попередньо обчислених значень та тимчасових

результатів. Функціональні блоки суматора, віднімача, помножувача та інверсії представляють арифметичні функції, що виконуються АС. Функція порівняння з 0 використовується при аналізі результатів виконання операцій в полі Галуа.

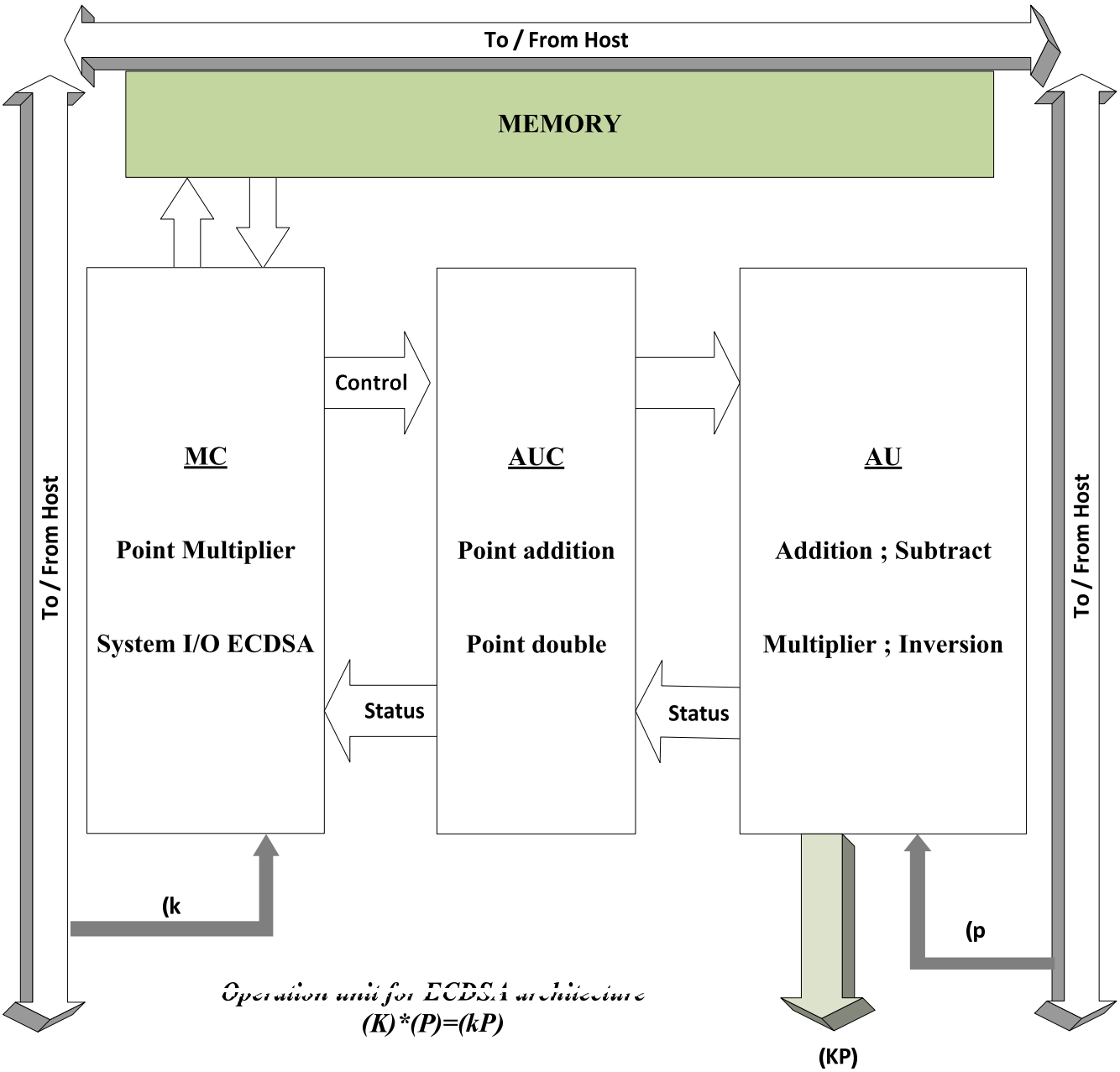



Рис. 4.1. Модель операційного вузла для ECDSA

4.2.3. Багаторівнева модель ядра

Опрацювання цифрових підписів на основі використання еліптичних кривих (ECDSA) - це декілька рівнів математичних операцій, пов'язаних з блоком керування відповідно до правил алгоритму ECDSA, рис. 2.3. Перші два рівні - це основні операції у полі Галуа: додавання GF, віднімання GF, множення GF, інверсія GF. Наступні два рівні - операції над точками еліптичних кривих: скалярне

множення точки на число, додавання та подвоєння точок, ці операції виконуються на рівні керування арифметичним вузлом. Верхній рівень - це ECC протокол ECDSA рівня.

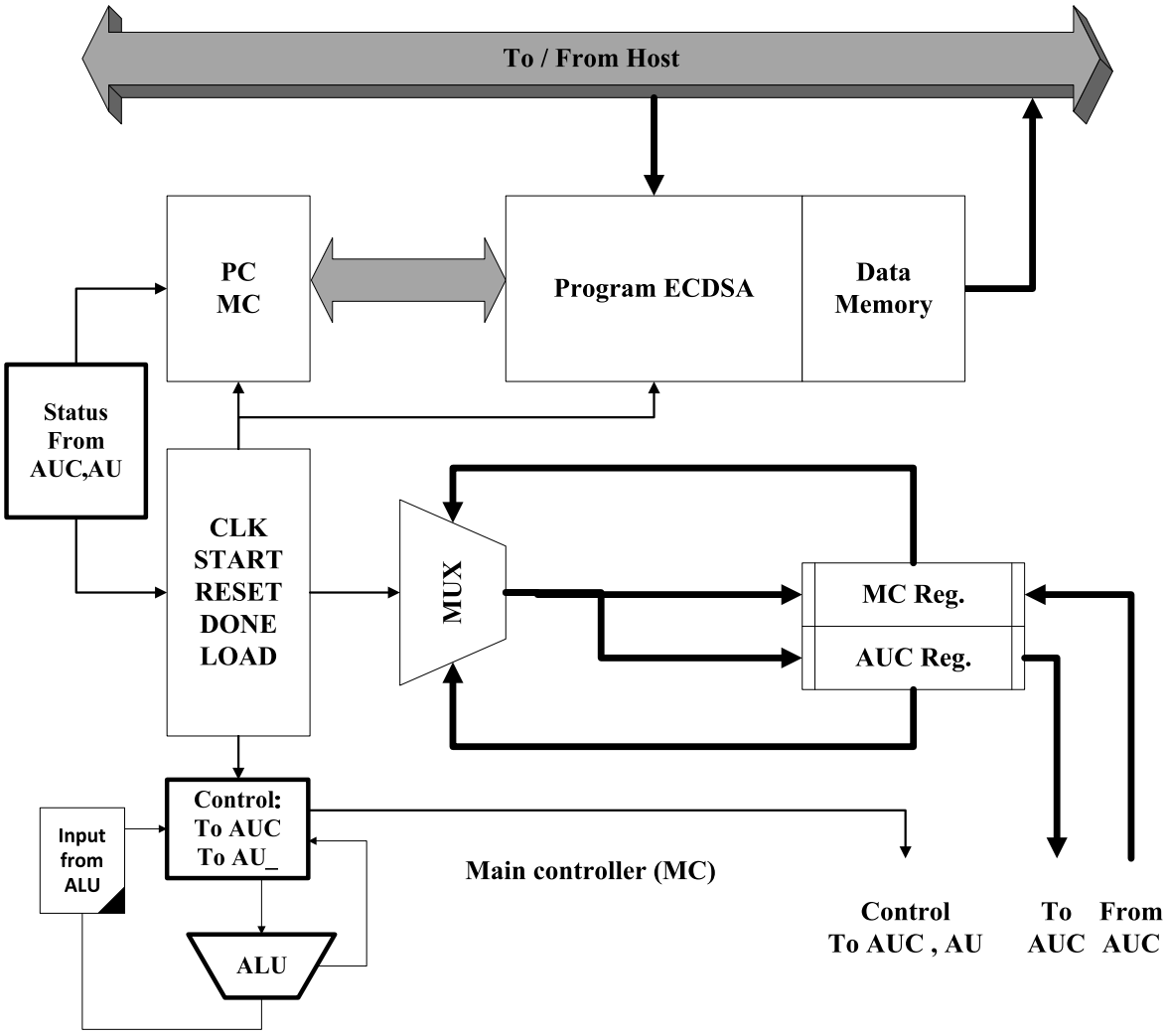



Рис. 4.2. Головний контролер (MC)

Первинно в моделі (рис. 4.1) було реалізовано алгоритми виконання основних операцій у поліноміальному базисі у двійкових розширених полях Галуа.

Один з алгоритмів множення, що починається з молодших розрядів множника, алгоритм обчислює c (x) = a (x) * b (x) mod f (x), де f (x) - незвідний поліном, що утворює поле, реалізацію алгоритму показано на рис. 4.5.

Algorithm 2 : Interleaved multiplication, LSB-first

*Input*: $A(x)=\sum_{i=0}^{m-1} a_i\alpha^i$, $B(x)=\sum_{i=0}^{m-1} b_i\alpha^i$, $a,b\in GF(2)$.

*Output* : $c(x)=\sum_{i=0}^{m-1} c_i\alpha^i; = A(x)\,B(x)\,mod\,f(x)$.

$1: c(x) \leftarrow 0; R(x) \leftarrow a(x);$

$2: For\ i\ in 0\ to 172 (or\ m-1\ genaral)\ do$

$3: c(x) := c(x) + bi\ \ R(x);$

$4: R(x) := a(x)\ \ x\ mod\ f(x)\ \ ; End\ loop;$

Піднесення до квадрату: піднесення до квадрату у полі $GF(2^{173})$ елемента a$(x)$ виконується як $c(x) = a(x)^2 \mod f(x)$ відповідно до наступної схеми обчислень, де $f(x)$ - незвідний поліноми поля:

$$d(x) = a^2(x) = \left(a_{m-1}x^{m-1} + \ldots + a_0\right)^2 = a_{m-1}x^{2(m-1)} + a_{m-2}x^{2(m-2)} \ldots + a_1x^2 + a_0.$$

$Thus\ d_i = a_{i/2}\ if\ i\ is\ even\ ,\ else\ d_i = 0.$

$$c_j = a_{j/2} + \sum_{\substack{0<i<m-2 \\ m+i\ even}} r_{ji} a_{(m+i)/2,} \quad j = 0,2,4\ldots$$

$$c_j = \sum_{0<i<m-2} r_{ji} a_{(m+i)/2,}\ j = 1,3,5\ldots.$$

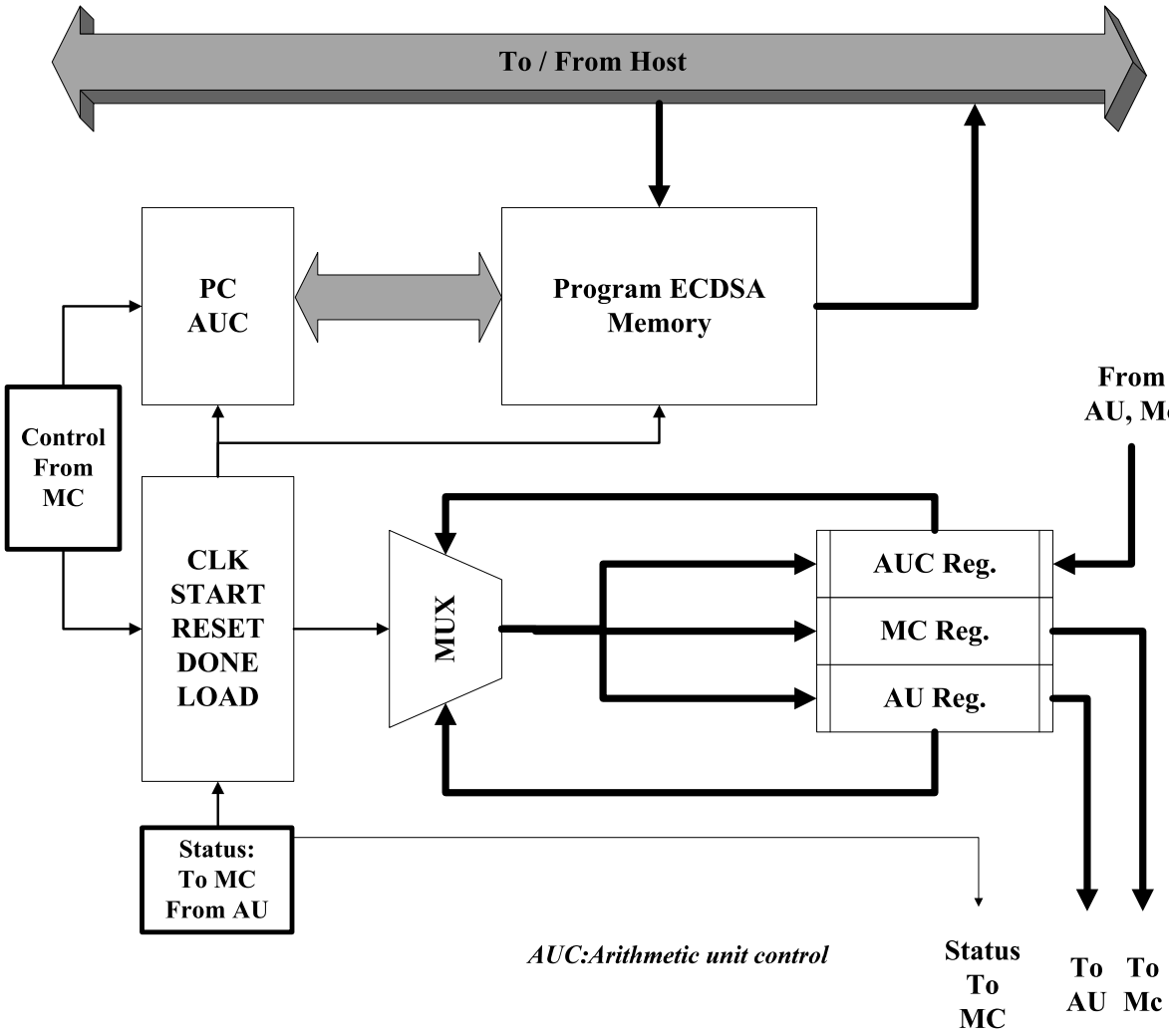



Рис. 4.3. Контролер арифметичного вузла (AUC)

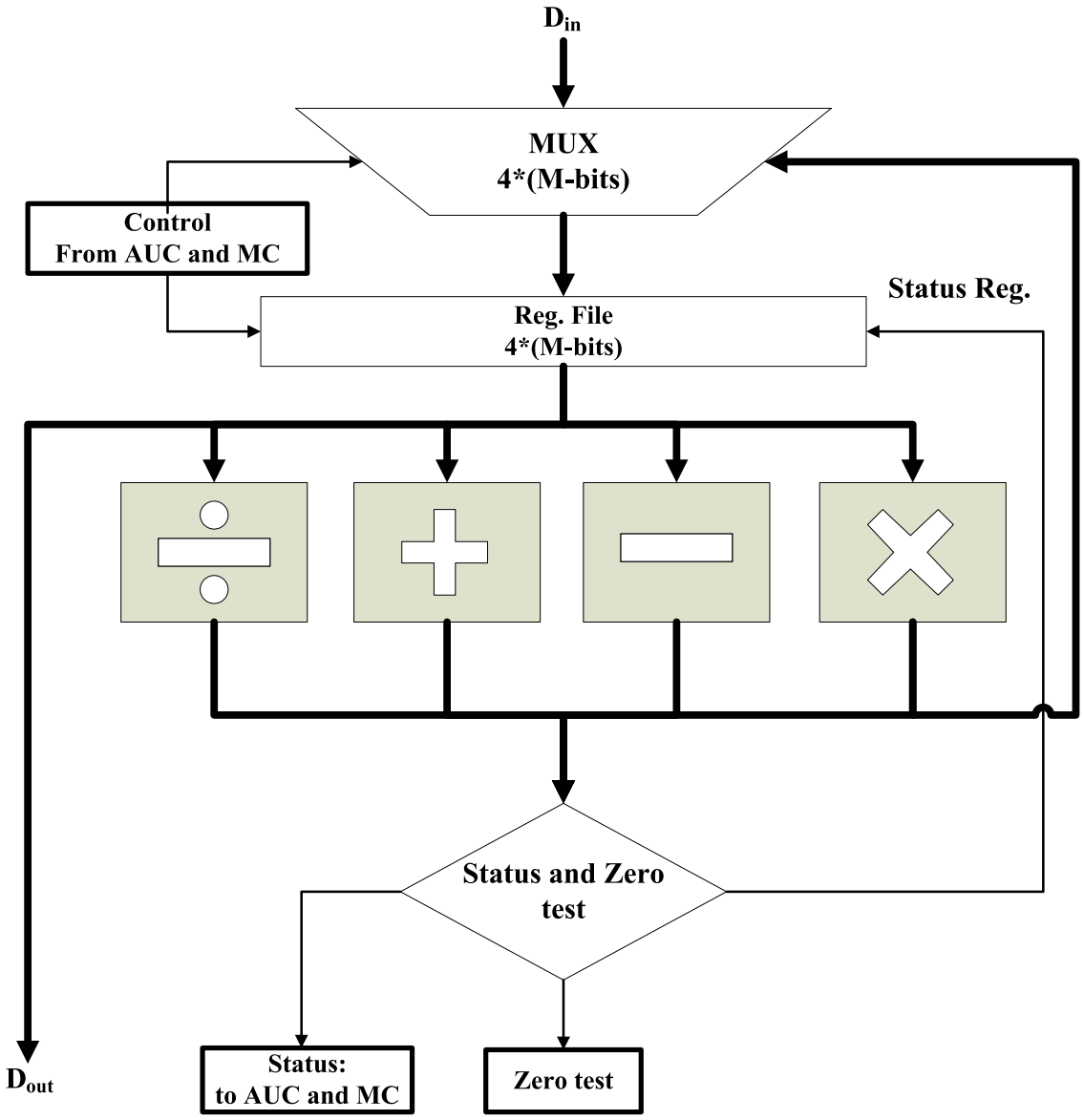



Рис. 4.4. Структурна схема арифметичного блоку

Ділення (знаходження оберненого елемента, інвертування, рис. 4.6) - це найбільш трудомістка операція в полі Галуа, оскільки воно використовує мультиплікативну інверсію (знаходження оберненого елемента): z(x) =g(x)*h(x)$^{-1}$modf(x); де h(x)$^{-1}$ = 1/h (мультиплікативна інверсія). Якщо g(x)=1, тоді z(x) є інверсією до h(x).

**Алгоритм 3:** двійковий алгоритм ділення $g(x)/h(x) modf(x)$

*Input* $a(x) := f(x)$; $b(x) := h(x)$; $u(x) := 0$; $v(x) := 1$ *or* $g(x)$;

*output: z(x)*

$\alpha := m$; $\beta := m - 1$

*while* $\beta \geq 0$ *loop*

$$if\ b_0 = 0\ then\quad b(x) := \frac{b(x)}{x};\ \ v(x) := v(x)x^{-1}\ mod\ f(x);\ \ \beta := \beta - 1$$

$$else\ if\quad \alpha > \beta\ then\ (a(x),\ b(x),\ u(x),\ v(x)) := (b(x), (a(x) + b(x))/x, v(x), (u(x) + v(x))x^{-1} mod\ f(x));$$

$$(\alpha,\ \beta) := (\beta,\ \alpha - 1);$$

$$else\ (b(x) := (a(x) + b(x))/x, v(x) := (u(x) + v(x))x^{-1} mod\ f(x); \beta := \beta - 1\ ; end\ if\ );$$

$$end\ loop;$$

Для знаходження мультиплікативної інверсії використано наступний алгоритм

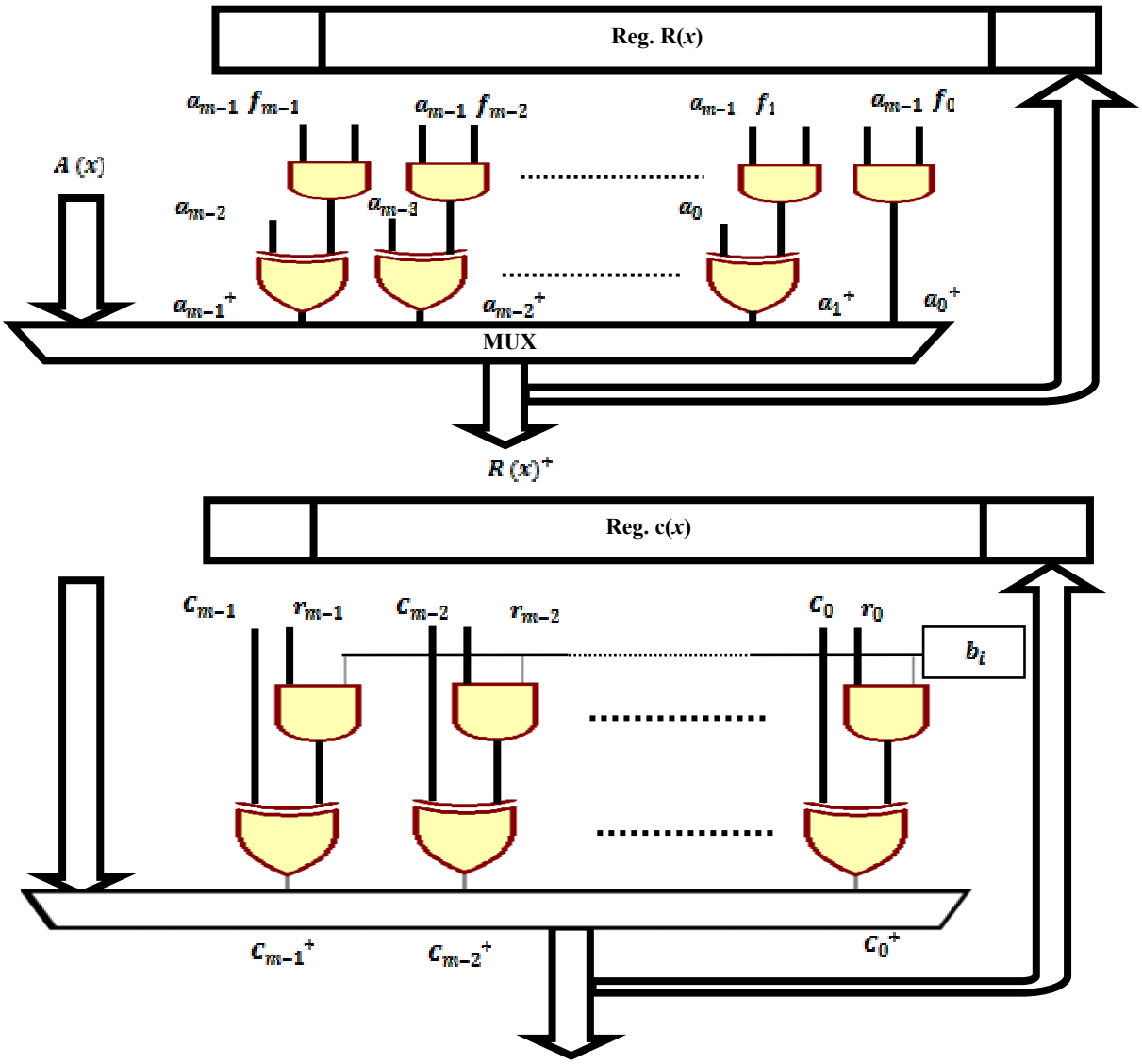



Рис. 4.5. Помножувач з накопиченням, виконує операції c(x) :=c(x) +bi *R(x);

R(x):=a(x)*x mod f(x)

**Алгоритм 4**: Алгоритм двійкової інверсії

Input: $f(x), a \in GF(2^m)$.

Output: $a^{-1} \bmod f(x)$.

*1.* $u \leftarrow a$, $v \leftarrow f(x)$, $A \leftarrow 1$, $C \leftarrow 0$

*2. While* $u > 0$ *do*

*2.1 While u is even do :*

$u \leftarrow u/2$ . If A is even then $A \leftarrow A/2$; *else* $A \leftarrow (A + f(x))/2$

*2.2 While v is even do :*

$v \leftarrow v/2$. If C is even then $C \leftarrow C/2$; *else* $C \leftarrow (C + f(x))/2$

*3. If* $u \geq v$ *then* $u \leftarrow u - v$, $A \leftarrow A - C$; *else* $v \leftarrow v - u$, $C \leftarrow C - A$.

*4. Return (C mod f(x))*

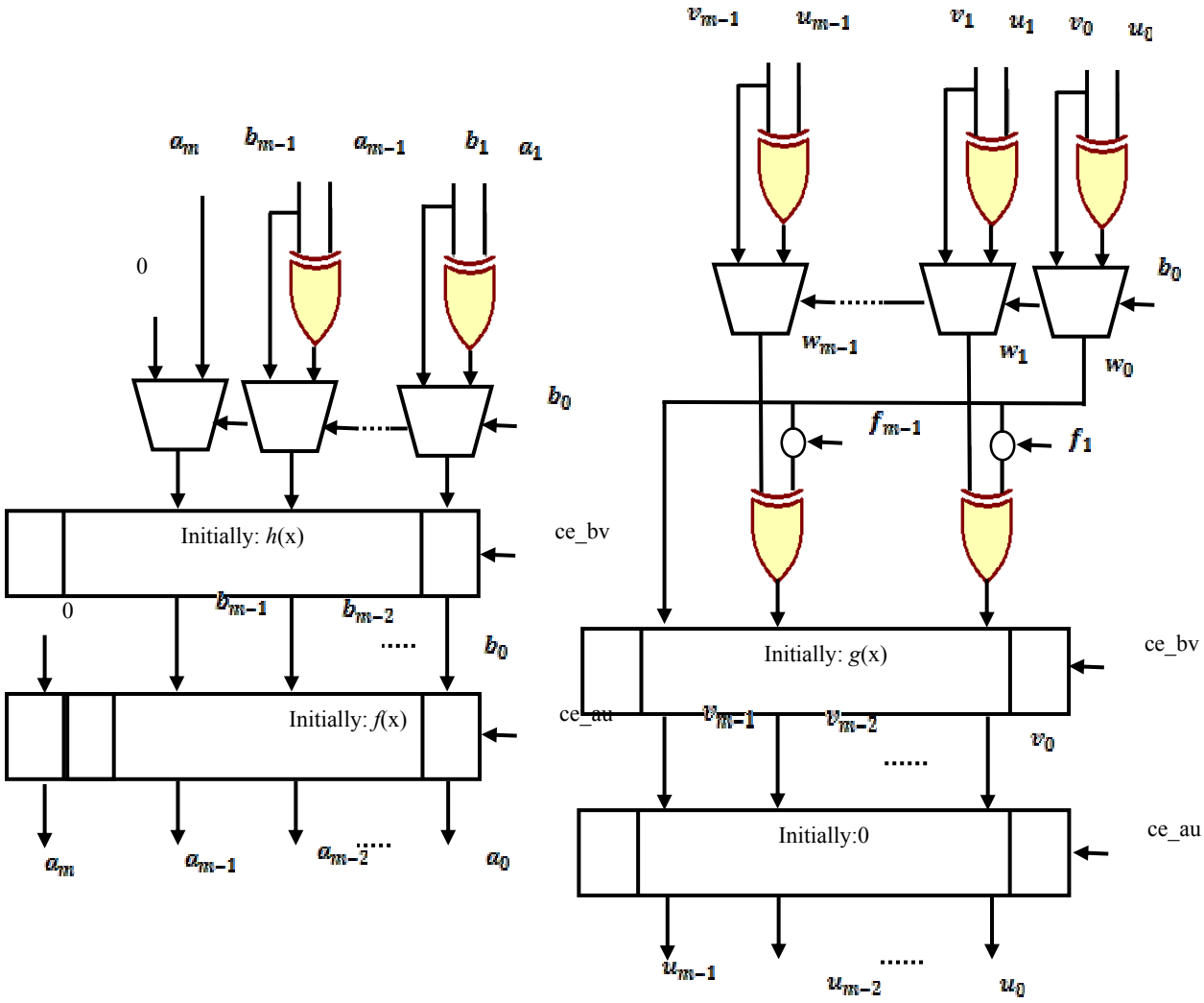



Рис. 4.6. Реалізація двійкового алгоритму ділення многочленів

4.2.4. Експериментальне дослідження створених вузлів та його результати

Експериментальне дослідження проводилося шляхом моделювання роботи розроблених ядер, в результаті чого було отримано їхні часові параметри (часову складність).

Апаратна складність визначалася за результатами імплементації розроблених ядер у ПЛІС.

Первинно, у цій роботі використовувалося поле $GF(2^{173})$ та поліноміальний базис, розрядність кодів елементів складала m=173 біта. На цьому етапі в пристрої було реалізовано m-бітні входи та виходи, для подачі операндів і аналізу проміжних та кінцевого результату, часові характеристики не вважалися суттєвими на цьому етапі роботи. Часові характеристики роботи арифметичного вузла наведено в таблиці 4.1. Часові характеристики подвоєння і додавання точок еліптичних кривих наведено у таблицях 4.2 та 4.3. Часові характеристики множення точок еліптичних кривих наведено у таблиці 4.4.

Максимальні досягнуті робочі частоти при опрацюванні елементів різних полів Галуа, що згадуються у [93], наведено у таблиці 4.5.

*Таблиця 4.1*

**Часові характеристики арифметичного вузла**

| FF-Level Operation | Clock Cycles |
|---|---|
| FF-Mult. | 173 |
| FF-Add. | 1 |
| FF-inver. | 346 |

*Таблиця 4.2*

**Часові характеристики операції подвоєння точок еліптичної кривої**

| Operation name | Operation number | Clock Cycles |
|---|---|---|
| INV | 1 | 346 |
| MUL | 2 | 346 |
| ADD | 3 | 3 |
| Total | | 695 |

*Таблиця 4.3*

**Часові характеристики операції додавання точок еліптичної кривої**

| Operation name | Operation number | Clock Cycles |
|---|---|---|
| INV | 1 | 346 |
| MUL | 2 | 346 |
| ADD | 5 | 5 |

| | |
|---|---|
| Total | 697 |

*Таблиця 4.4*

**Часові характеристики операції скалярного множення точок еліптичної кривої**

| Operation | Clock Cycles |
|---|---|
| EC-Double | 695 |
| EC-Add | 697 |
| k·P | 121,100 |

*Таблиця 4.5*

**Максимальні робочі частоти для різних полів Галуа**

| GF | MAX _Frequency |
|---|---|
| $GF(2^{233})$ | 136.323 MHz |
| $GF(2^{173})$ | 142.857 MHz |
| $GF(2^{163})$ | 169.477 MHz |

4.2.5. Модифікація стенда для роботи у трійкових полях Галуа

Запропонований і розроблений стенд було модифіковано для дослідження ядер опрацювання елементів розширених полів Галуа $GF(p^m)$ з характеристиками $p > 2$, в першу чергу з характеристикою $p = 3$, використання яких може бути перспективним в найближчому майбутньому (п. 1.6.5).

Для дослідження доцільності використання різних полів аналізувалися поля з приблизно однаковим порядком, на першому етапі з порядком приблизно рівним $2^{173}$.

*Таблиця 4.6*

**Розширені поля Галуа з приблизно однаковим порядком**

| Поле | Кількість біт в коді елемента | Кількість цифр в коді елемента | Кількість біт в коді цифри | Діапазон значень цифр коду елемента |
|---|---|---|---|---|
| $GF(2^{173})$ | 173 | 173 | 1 | 0-1 |
| $GF(3^{87})$ | 174 | 87 | 2 | 0-2 |
| $GF(7^{58})$ | 171 | 57 | 3 | 0-6 |
| $GF(13^{43})$ | 172 | 43 | 4 | 0-12 |
| $GF(31^{34})$ | 170 | 34 | 5 | 0-30 |
| $GF(61^{28})$ | 168 | 28 | 6 | 0-60 |
| $GF(127^{24})$ | 168 | 24 | 7 | 0-126 |
| $GF(251^{21})$ | 168 | 21 | 8 | 0-250 |
| $GF(251^{5})$ | 40 | 5 | 8 | 0-250 |

Робота із створення вузлів, що опрацьовують елементи таких розширених полів Галуа, виявила суттєву умову, яка дозволила розв’язати задачу порівняння вузлів для різних полів – розширені поля Галуа повинні бути з приблизно

однаковою кількістю елементів.

Аналіз результатів ДБ Кібер привів до необхідності теоретично їх узагальнити та обґрунтувати використання того чи іншого розширеного поля Галуа, тобто, порівнювати операційні вузли для цих полів. Внаслідок цього було розроблено метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ і, як його частини, - методи оцінювання часової [п. 2.10], структурної [п. 2.11], ємнісної [п. 2.12] складностей помножувачів елементів розширених полів Галуа та метод оцінювання складності злому апаратних засобів КЗІ [п. 2.13].

4.3. Впровадження результатів на ф. Al Nabaa Network solutions (Багдад, Ірак).

Впровадження результатів на ф. Al Nabaa Network solutions (Багдад, Ірак) підтверджено Актом (Додаток Б). До основних результатів роботи, які було використано на ф. Al Nabaa Network solutions (Багдад, Ірак) і які дозволили покращити технічні рішення фірми належать:

використання цифрових підписів для забезпечення безпеки (п. 1.4.2, п. 3.1);

висока продуктивність запропонованих для використовування алгоритмів (п. 3.4.1, п. 3.5);

ефективність та функціональність помножувачів (п. 2.10.4);

ефективність та функціональність знаходження мультиплікативної інверсії (п. 3.2, п. 3.5);

рівень протидії злому даних (п. 2.11, п. 2.13);

вбудоване тестування (п. 2.14).

4.4. Впровадження в навчальний процес Національного університету «Львівська політехніка».

Результати дисертаційного дослідження використано на кафедрі електронних обчислювальних машин Інституту комп’ютерних технологій автоматики та метрології (ІКТА) Національного університету «Львівська політехніка» при підготовці і проведенні курсу лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп’ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп’ютерна інженерія»,

спеціалізації «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»), що підтверджено Актом (Додаток В).

У впроваджених в навчальний процес розроблених методичних вказівках до лабораторної роботи [22] наведено теоретичні відомості про розширені поля Галуа (р. 1.5), про модифіковані комірки Гілда (п. 2.9.2, рис. 2.4) та запропоновані в роботі помножувачі на їх основі (п. 2.9.2, рис. 2.5, рис. 2.6), наведено VHDL-описи модифікованої комірки Гілда та основних елементів помножувача (Додаток П).

У методичних вказівках, як взірець, наведено функціональну схему помножувача елементів полів Галуа $GF(3^4)$ (рис. 4.7) і варіанти утворюючих поле поліномів та операндів, над якими необхідно виконати множення. Студенти повинні модифікувати схему та VHDL-описи елементів, промоделювати роботи виправленої схеми і продемонструвати правильний результат.

Варіанти утворюючих поліномів [138] наведено нижче.

Прості поліноми P, які утворюють поле $GF(3^2)$

112

122

Прості поліноми P, які утворюють поле $GF(3^3)$

1021 ($1*x^3+0*x^2+2*x^1+1*x^0 = x^3+2x+1$)

1121

1201

1211

Прості поліноми P, які утворюють поле $GF(3^4)$

10012

10022

11002

11122

11222

12002

12112

12212

Пояснення роботи, особливостей дослідження та проєктування описаних в методичних вказівках вузлів введено в лекційний курс «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія».

4.5. Висновки до розділу 4

*У четвертому розділі описано* експериментальне дослідження та впровадження розроблених операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

*Основний результат: створено генератор ядер* для знаходження у поліноміальному базисі мультиплікативних інверсій елементів двійкових полів Галуа $GF(2^m)$ для визначених стандартами степенів (до $m = 998$), які використовуються при опрацюванні цифрових підписів на основі еліптичних кривих.

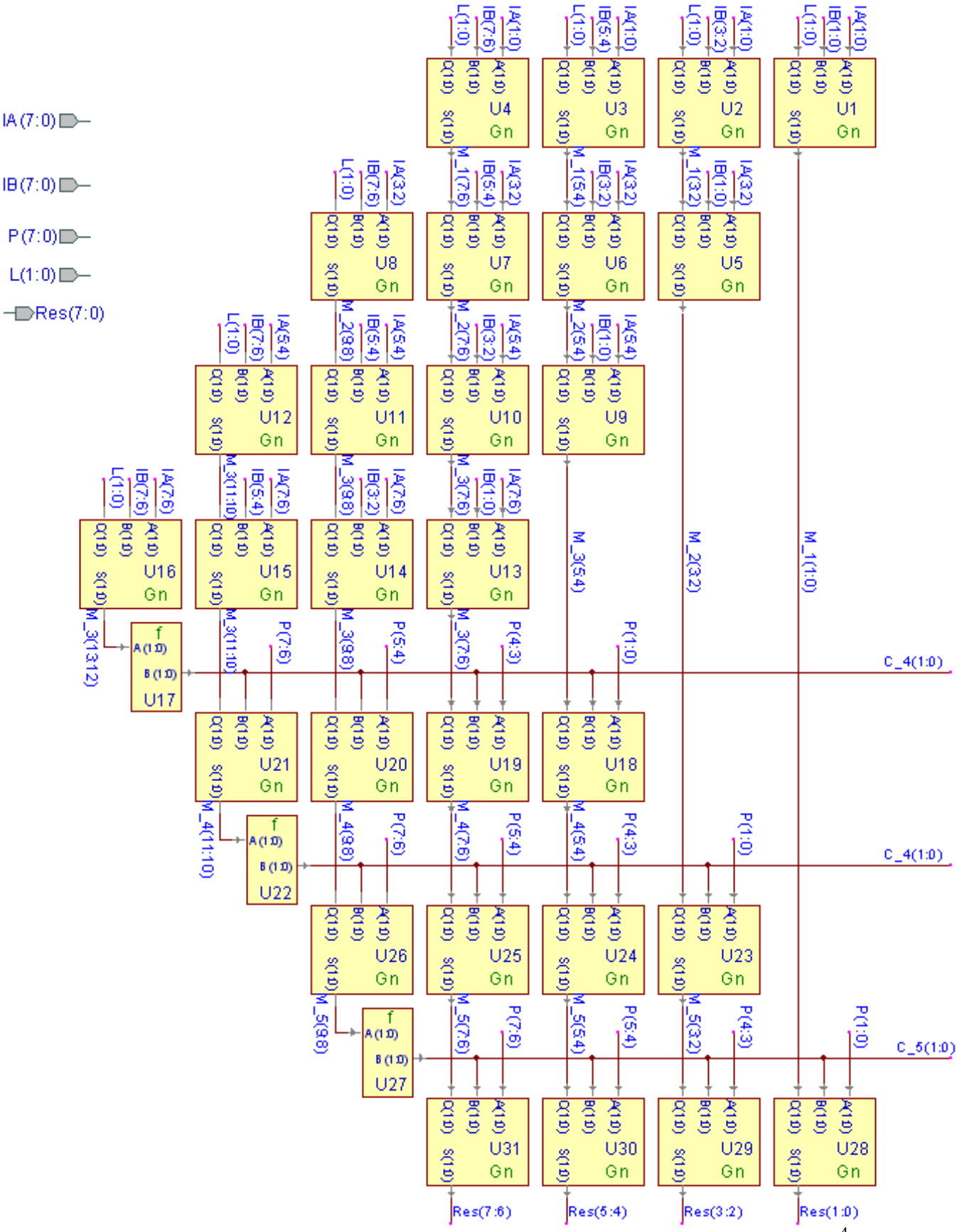



Рис. 4.7. Функціональна схема помножувача елементів поля GF($3^4$)

*Роботу генератора перевірено на рівні моделей для m = 163, 173, 233 (які вимагалися для першочергового впровадження) та в інших розширених полях*

*(*$GF(3^{87})$, $GF(7^{58})$, $GF(13^{43})$, $GF(31^{34})$, $GF(61^{28})$, $GF(127^{24})$, $GF(251^{21})$, $GF(251^{5})$*) з кількістю елементів, що приблизно дорівнює* $2^{173}$.

Аналіз розширених полів Галуа з приблизно однаковою кількістю елементів – найважливіша риса запропонованих методів порівняння операційних вузлів, що опрацьовують елементи цих полів.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом) (Додаток А, Додаток Б).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»), що підтверджено відповідним Актом.

# ВИСНОВКИ

У ході виконання роботи досягнуто поставлено мету. На основі проведених досліджень здійснено наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів, розв'язано важливе наукове завдання створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які працюють з елементами розширених полів Галуа *GF(pm),* розроблено структурні алгоритми їх роботи. При цьому розв'язано такі взаємозв'язані задачі і отримано такі нові наукові результати.

проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП), що дозволило сформулювати мету роботи і завдання дослідження;

визначено основні архітектурні принципи побудови та розроблено узагальнену модель операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розроблено метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ та метод оцінювання складності злому апаратних засобів КЗІ;

вдосконалено метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі;

створено і апробовано технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

створено та перевірено уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

визначено найкращі для використання розширені поля Галуа, за сукупністю показників найращим є розширене поле з характеристикою 3;

проведено експериментальне дослідження та впровадження розроблених операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

Отримані у дисертаційній роботі наукові результати створюють методологічну базу для розроблення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом) (Додаток А, Додаток Б).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп’ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп’ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп’ютерна інженерія», спеціальностей «Комп’ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»).

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

*1. Алферо А. П., Зубо А. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии. М.:Гелиос АРВ, 2002. 2-е изд.*

*2. Баричев С.Г. и др. «Основы современной криптографии». – М.: «Горячая линия – Телеком», 2001 – 120 с.*

*3. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгебраические и алгоритмические основы: Элементарное введение в эллиптическую криптографию. Издательство: КомКнига, 2006. 328 с.*

*4. М. Бондаренко, Иван Горбенко, Андрей Свинарев, Александр Столяр, Виктор Лапин. Принципы построения и использования аппаратных средств защиты информации серии "Гряда". Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

*5. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. — М.:МЦНМО, 2003.—328 с.*

*6. Глухов В.С. Система команд криптографічного процесора // Вісник Національного університету "Львівська політехніка" "Комп`ютерні системи та мережі". Вип. 523. Львів, 2004.*

*7. Глухов В.С. Особливості виконання операцій над матрицями в полях Галуа // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". Вип. 564. Львів, 2006. С.35-39.*

*8. Глухов В.С. Обчислювальний пристрій для операцій над еліптичними кривими // Вісник Національного університету "Львівська політехніка" "Комп`ютерні системи та мережі". № 573. Львів, 2006. С.54-61.*

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

*10. В.С. Глухов. Вдосконалення алгоритму обчислення оберненого елемента $GF(2^t)$ в нормальному базисі // Вісник Національного університету "Львівська політехніка" "Комп`ютерні системи та мережі". №603. Львів, 2007. С.20-26.*

*11. Глухов В.С. Багаторівнева організація операційного пристрою для роботи з елементами поля Галуа, представленими у нормальній формі. Збірник матеріалів міжвузівської науково-технічної конференція науково-педагогічних працівників «Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні» . - Львів: Ліга-Прес. 2007.*

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

*13. Глухов В.С. Вибір багатоядерних структур для пристроїв обробки ЕЦП // Вісник Національного університету "Львівська політехніка" "Комп`ютерні системи та мережі". № 658. Львів, 2009. С.35 – 39.*

*14. Глухов В.С. Вбудований контроль множення в гаусівському нормальному базисі типу 2 полів Галуа $GF(2^m)$. Науково-технічний журнал «Радіоелектронні і комп'ютерні системи 6(47). Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут». Харків. «ХАІ». 2010. С. 255 – 259.*

*15. Глухов В.С. Оцінювання апаратних витрат на реалізацію багаторівневої комп'ютерної системи з врахуванням закону Амдаля // Вісник Національного університету «Львівська політехніка» «Комп'ютерні науки та інформаційні технології» № 663. Львів, 2010. С.17 - 23.*

*16. Глухов В.С. Особливості виконання операцій у простих полях Галуа GF(p) у сучасних засобах захисту інформації // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі", № 717. Львів, 2011. С.3 -9.*

*17. В.С.Глухов, Т.С.Берко. Перевірка пристроїв для обробки ЕЦП, що ґрунтуються на еліптичних кривих / Науково-соціальний часопис "Технічні вісті". Орган Українського інженерного товариства у Львові, 2007/1(25), 2(26), с. 53-57.*

*18. 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.*

*19. В. С. Глухов, В. А. Голембо. Методичні вказівки до курсової роботи "Арифметичні та логічні основи комп'ютерних технологій" з дисципліни "Комп'ютерна логіка". Львів: Видавництво Еаціонального університету "Львівська політехніка", 2014.*

*20. Глухов В. С., Еліас Р. М., Мельник А. О. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа GF($2^m$) з надвеликим степенем [Текст] / В.С. Глухов., Р.М. Еліас, А.О. Мельник // "Комп'ютерно-інтегровані технології:освіта, наука, виробництво" - науковий журнал, Луцький національний технічний університет. – Луцьк: 2013. - № 12. - С. 103 – 106.*

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

*22. Глухов В.С., Жолубак І.М., Костик А.Т, Рахма М.К.Р. Проектування і моделювання елементів комп'ютерних систем та мереж. Методичні вказівки до лабораторних робіт з дисципліни"Дослідження і проектування комп'ютерних систем та мереж" для студентів освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», Поліграфічний центр Видавництва Національного університету "Львівська політехніка". Львів. 2019. 118 с.*

*23. В. С. Глухов, А. Т. Костик. Використання сучасних ПЛІС для опрацювання елементів полів Галуа GF($p^q$). Дев'ята конференція ХУ ПС ім. І. Кожедуба, 17 – 18 квітня, 2013 року. Харків. 2013. С . 178.*

*24. В.Глухов, Н.Заіченко, Б.Оліярник. Спецпроцесор для бортових інформаційно-керуючих систем. Наукові нотатки. Міжвузівський збірник (за*

*напрямком «Інженерна механіка»), випуск 19 (січень 2007). Луцький державний технічний університет, Луцьк. 2007. С.33-43.*

*25. Глухов В.С., Ногаль М.В. Спеціалізований однорозрядний процесор для захисту інформації в гарантоздатних системах. Науково-технічний журнал «Радіоелектронні і комп'ютерні системи 5 (32). Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут». Харків. «ХАІ». 2008. С. 104-109.*

*26. 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.*

*27. Глухов В.С., Элиас Р. Уменьшение структурной сложности многосекционных умножителей элементов полей Галуа. / В.С.Глухов, Р.Элиас // Электротехнические и компьютерные системы. - 2015. - № 19(95) - С. 222-226.*

*28. 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. АСІТ'2015. 22-23 травня 2015 року. Тернопіль. ТНЕУ. 2015. С. 166 – 167.*

*29. Горбенко І. Д., Гріненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. спец. "Комп'ютерні науки", "Комп'ютена інженерія", "Прикладна математика", "Інформаційна безпека" вищ. навч. закл. / Харківський національний ун-т радіоелектроніки. - Х. : ХНУРЕ, 2004. - Бібліогр.: с. 364-368. Ч. 1 : Криптографічний захист інформації. - 368с. : рис. - ISBN 966-659-081-6.*

*30. Горбенко І. Д. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнєцов, О. В. Потій, Ю. І. Горбенко, Р. С. Ганзя, В. А. Пономар // Радиотехника. - 2016. - Вып. 186. - С. 32 - 52.*

*31. І. Д. Горбенко, В. А. Пономар. Дослідження можливості використання і переваг постквантових алгоритмів в залежності від умов застосування. Восточно-Европейский журнал передовых технологий. Информационно-управляющие системы. 2/9 ( 86 ) 2017. ISSN 1729-3774 . С. 21-32.*

*32. Горбенко Ю. И., Ганзя Р. С. Анализ стойкости постквантовых криптосистем / Ю. И. Горбенко, Р. С. Ганзя // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 268–274.*

*33. Грушо А. А. Тимонина Е. Е. Теоретические основы защиты информации. Издательство Агентства "Яхтсмен". 1996 г. http://kiev-security.org.ua.*

*34. С. Гудман, С. Хидетниеми. Введение в разработку и анализ алгоритмов. Издательство «Мир». Москва. 1981.*

*35. Б. П. Демидович и И. А. Марон. Основы вычислительной математики. Издание четвертое, исправленное и дополненное. Издательство «Наука». Главная редакция физико-математической литературы. Москва. 1970.*

*36. А. Добуш. Збільшення степеня основного поля Галуа для цифрових підписів. Тези доповідей V міжнародної науково-технічної конференції "Комп'ютерні системи та мережні технології CSNT 2012". С. 48. м. Київ 13-15 червня 2012 р.*

*37. Домарев В. В. Безопасность информационных технологий. Системный подход. Издательство ТИД "ДС", 2004 г., 992 стр. ISBN 966-7992-36-5*

*38. Дудикевич В. Б. Парадигма та концепція побудови багаторівневої комплексної системи безпеки кіберфізичних систем / В. Б. Дудикевич, В. М. Максимович, Г. В. Микитин // Вісник Національного університету «Львівська політехніка». Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 3–7. – Бібліографія: 8 назв.*

*39. Еліас Р. Убудований контроль спецпроцесорів для опрацювання ЕЦП. / Глухов В. С. Еліас Р. // Комп'ютерні науки та інформаційні технології. / Л. : Вид-во Нац. ун-ту "Львів. політехніка", 2010. – С. 56 - 62.– (Вісник / Нац. ун-т "Львів. політехніка"; № 686.*

*40. Еліас Р. Засоби відлагодження пристроїв з вбудованим контролем для*

*опрацювання елементів полів Галуа GF($2^m$). / Глухов В., Еліас Р. // Комп`ютерні системи та мережі. / Л. : Вид-во Нац. ун-ту "Львів. політехніка", 2010. – С. 70 - 76. – (Вісник / Нац. ун-т "Львів. політехніка"; № 688.*

*41. Р. Еліас. Особливості синтезу генератора ядер секціонованих помножувачів елементів полів Галуа GF($2^m$) для пристроїв обробки цифрових підписів. / В. Глухов, Р. Еліас. // І Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем". 31 травня - 01 червня 2012 р. Львів, Україна.*

*42. Еліас Р. Генератор ядер секціонованих помножувачів елементів полів Галуа GF($2^m$) для оптимального нормального базису 2-го типу. / Глухов В., Еліас Р. // Комп'ютерні науки та інформаційні технології. / Л. : Вид-во Нац. ун-ту "Львів. політехніка", 2012. – С. 78 - 84. – (Вісник / Нац. ун-т "Львів. політехніка"; № 732.*

*43. Рахма, М. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Р. М. Еліас, В. С. Глухов, М. Рахма, І. М. Жолубак / Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 905. Львів, 2018. С. 64-72*

*44. Р. Еліас, М. Рахма, В.С. Глухов. Часова складність помножувачів для полів Галуа. Програма 2-ої Міжнародної науково-технічної конференції «Електротехнічні і комп'ютерні системи: теорія і практика (Елтекс 2016)» м. Одесса, 26–28 червня 2016 р.*

*45. Р. Еліас, М. Рахма, В. Глухов. Зменшення структурної складності багатосекційних помножувачів елементів полів Галуа. Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика (ЕЛТЕКС-2017)». Одеса, Одеський національний політехнічний університет. 26 – 28 червня 2017 р.*

*46. В. Ємець, А. Мельник, Р. Попович. Сучасна криптографія. Основні поняття. – Львів: БаК, 2003. - 144 с.*

*47. 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.*

*48. Жолубак, І. М., Глухов, В. С. Дослідження апаратної складності помножувачів розширених полів Галуа GF($d^m$). Кіберфізичні системи: досягнення та виклики. – 2016 р. Матеріали II Наукового семінару, 21–22 червня 2016 року, Львів. С. 98 – 104.*

*49. І. М. Жолубак, А. Т. Костик, В. С. Глухов. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі [Текст] / І. М. Жолубак, А. Т. Костик, В. С. Глухов // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів: - 2015. - Вип. 830. - С. 27 - 33.*

*50. Коблиц Н. «Курс теории чисел и криптографии». - 2001. Москва: Научное изд-воТВП, 2001*

*51. Т. Коркішко, А. Мельник, В. Мельник. Алгоритми та процеси симетричного блокового шифрування. – Львів: БаК, 2003. - 168 с.*

*52. Коркішко Т.А., Мельник А.О. Вимоги до продуктивності процесів шифрування симетричними блоковими алгоритмами // Вісник Національного університету "Львівська політехніка" № 437 «Комп'ютерні системи та мережі». Львів. Видавництво Національного університету «Львівська політехніка». 2001. С.83– 90.*

*53. Кочубинский А.И. Эллиптические кривые в криптографии. //Безопасность информации. – 2, - 2000, с. 18 – 31. www.bitis.com.ua:8080/downloads/elliptica.doc*

*54. В. Я. Крайовський, А. О. Мельник. „Вплив компонент архітектури програмованого комп'ютерного пристрою на його характеристики" // Вісник Національного університету «Львівська політехніка» «Комп`ютерні системи та мережі» № 630. Львів, 2008. С.76-81.*

*55. А. А. Кузнецов, А. В. Потий, Н. А. Полуяненко, И. В. Стельник. Нелінійні*

*функції ускладнення для потокових симетричних шифрів. Радіотехніка. Т.4, № 195, 2018. С. 125 - 137*

*56. Г. В. Кузнецов, В. В. Фомичов, С. О. Сушко, Л. Я. Фомичова. Математичні основи криптографії. Навч. посібник. Дніпропетровськ. Національний гірничий університет, 2004 - Ч. 1. - 391 с.*

*57. Мелащенко А. О., Перевозчикова О. Л. Национальная система электронных цифровых подписей как открытая система / Кибернетика и системный анализ – 2011.*

*58. Мельник А. О. Архітектура комп'ютера. Підручник. – Луцьк: Волинська обласна друкарня, 2008. – 470 с.*

*59. Мельник А. О., Коркішко Т. А. Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів // Вісник Державного університету "Львівська політехніка" № 385 «Комп'ютерні системи та мережі». Львів. Видавництво Державного університету «Львівська політехніка». 2000. С. 77 – 80.*

*60. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку / А. О. Мельник // Вісник Національного університету "Львівська політехніка". – 2014. – № 806 : Комп'ютерні системи та мережі. – С. 154–161. – Бібліографія: 31 назва.*

*61. Мельник А. О. Хамелеон - система високорівневого синтезу спеціалізованих процесорів / А. О. Мельник, А. М. Сало, В. Клименко, Л. Цигилик, А. Юрчук // Радіоелектронні і комп'ютерні системи. - 2009. - № 5. - С. 189–194. - Режим доступу: http://nbuv.gov.ua/UJRN/recs_2009_5_37.*

*62. Мельник А. О., Мельник В. А. Персональні суперкомп'ютери: архітектура, проектування, застосування. Монографія. Львів: Видавництво Львівської політехніки, 2013. 516 с.*

*63. Муттер В. М., «Основы помехоустойчивой телепередачи информации»- М.: Радио и связь, 1994. – 293 с.*

*64. Николайчук Я. М. Коди поля Галуа : теорія та застосування [Текст] : монографія / за ред. Я. М. Николайчука. – Тернопіль : ТзОВ "Терно граф", 2012. - 392 с.*

*65. Я. М. Николайчук, Н. Я. Возна, В. М. Грига, Б. Б. Круліковський, А. Я. Давлетова. Високопродуктивні матричні та потокові перемножувачі цифрових даних. Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. пр. — Кам'янець-Подільський: Кам'янець-Подільськ. нац. ун-т, 2019. — Вип. 19. — С. 101-107*

*66. Я. М. Николайчук, О. І. Волинський, П. В. Гуменний, Т. І. Пастух. Методи міжбазисних перетворень багаторозрядних кодів теоретико-числових базисів Радемахера–Крестенсона. Математичне та комп'ютерне моделювання. Серія: Технічні науки. Випуск 15. Інститут кібернетики ім. В. М. Глушкова НАН України. 2017. С. 143 – 149.*

*67. Николайчук, Я. М. Метод факторизации многоразрядных чисел на основе свойств квадратичности вычетов в системе остаточных классов / Я. Н. Николайчук, С. В. Ивасьев, И. З. Якименко, М. Н. Касянчук // Вестник Брестского государственного технического университета. – 2015. – № 5(95): Физика, математика, информатика. – С. 42–45.*

*68. О. В. Потій, К. В. Ісірова. Аналіз вимог та моделей безпеки для постквантової криптографії // Математичне та комп'ютерне моделювання. Серія: Технічні науки. Випуск 15. 2017. С. 192 – 197.*

*69. Рабинович З.Л., Раманаускас В.А. Типовые операции в вычислительных машинах. – К.: Техніка, 1980. – 264 с., ил.*

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

*71. Рахма, М. Структурна складність помножувачів елементів полів Галуа у нормальному та поліноміальному базисах / Р. Еліас, М. Рахма, В. Глухов / Електротехнічні та комп'ютерні системи. – Одеса: – 2017. Вид-во Наука і техніка. - № 25 (101). – С. 332-340.*

*72. Рахма, М. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Р. М. Еліас, В. С. Глухов, М. Рахма, І. М. Жолубак / Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 905. Львів, 2018. С. 64-72*

*73. Рахма, М. Ємнісна складність та вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Родріг Еліас, Валерій Глухов, Мохаммед Рахма, Іван Жолубак / Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 29(105), с. 95-102*

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

*75. Рахма, М. Аналіз можливості побудови багатосекційних помножувачів елементів полів Галуа для нормального та поліноміального базисів / В. С. Глухов, Р. Еліас, М. Рахма / Матеріали третього наукового семінару Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 13-14 червня 2017 р. С. 38-47.*

*76. Рахма, Мохаммед Кадім Рахма. Принципи побудови та проектування операційних вузлів для полів Галуа, що використовуються в задачах криптографічному захисті інформації на основі еліптичних кривих / В.С. Глухов, І.М. Жолубак, Мохаммед Кадім Рахма Рахма / Кіберфізичні системи: багаторівнева організація та проектування [Текст]: монографія – А.О. Мельник та інші. За редакцією професора А. О. Мельника. Львів: «Магнолія 2006», 2019. 238 с. С. 58-131.*

*77. Самофалов К.Г., Романкевич А.М., Валуйський В.Н., Каневський Ю.С., Пиневич М.М. Прикладная теория цифровых автоматов. – К.: Вища шк. Головное изд-во, 1987. – 375 с.*

*78. Г. Семенов. Цифровая подпись. Эллиптические кривые. Открытые*

*системы, #07-08/2002.*

*79. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.*

*80. Черкаський М.В. SH-модель алгоритму // Вісник Національного університету "Львівська політехніка" № 433. Видавництво Національного університету «Львівська політехніка». 2001. С.127 – 134.*

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

*82. Шапочка Н. В., Горбенко І. Д. Обґрунтування та визначення вимог до засобів криптографічного захисту інформації. Сборник трудов второй международной студенческой научно-технической конференции «Информатика и компьютерные технологии 2006» 13 декабря 2006 года. ДонНТУ. Донецк 2006.*

*83. Шологон О. З. Види загроз у кіберфізичних системах // Вісник Національного університету "Львівська політехніка" № 830 «Комп'ютерні системи та мережі». Львів. Видавництво Національного університету «Львівська політехніка». 2015. С.164 - 169.*

*84. 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.*

*85. 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.*

*86. Шологон Ю. З. Вразливості апаратного забезпечення кіберфізичних систем // Вісник Національного університету "Львівська політехніка" № 830 «Комп'ютерні системи та мережі». Львів. Видавництво Національного*

*університету «Львівська політехніка». 2015. С.164 - 169.*

*87. Аппаратная и программная реализация алгоритмов шифрования. http://cryptogrof.ru/apparatnaja_i_programtmnaja_realizacija_algoritmov_shifrovanija*

*88. Атака сторонніми каналами.*

*https://uk.wikipedia.org/wiki/Атака_сторонніми_каналами*

*89. ГОСТ 34.310-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997.*

*90. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хэширования. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997.*

*91. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*

*92. ГОСТ 28906-91 (ИСО 7498-84, ИСО 7498-84 Доп.1-84). Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель.*

*93. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. ЕЦП, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ. 2003.*

*94. ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Базова модель (ISO/IEC 7498-1:1994).*

*95. ДСТУ ISO-IEC 10118-1-2003. Інформаційні технології; Методи захисту. Геш-функції / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2004.*

*96. ДСТУ ISO/IEC 13888-1:2015. Інформаційні технології; Методи захисту. Неспростовність. Частина 1. Загальні положення (ISO/IEC 13888-1:2009, IDT)*

*97. ДСТУ ISO/IEC 14888-1:2015 Информационные технологии. Методы защиты. Цифровые подписи с дополнением. Часть 1. Общие положения (ISO/IEC 14888-1:2008, IDT)*

*98. ДСТУ ISO/IEC 15946-1:2015 Інформаційні технології. Методи захисту. Криптографічні методи, що грунтуються на еліптичних кривих. Частина 1. Загальні положення.*

*99. ДСТУ ISO/IEC 15946-3:2006 Інформаційні технології. Методи захисту. Криптографічні методи, що грунтуються на еліптичних кривих. Частина 3. Установлення ключів.*

*100. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення*

*101. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція хешування*

*102. Закон України «Про електронний ЕЦП» від 22.05.2003 № 852-IV (Відомості Верховної Ради (ВВР), 2003, N 36, ст.276)*

*103. Звіт про науково-дослідну роботу ДБ/КІБЕР (№ держреєстрації 0115U000446) «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кіберфізичних систем», розділ 9 «Захищений обмін, опрацювання та зберігання вимірювальної та службової інформації».*

*104. Метод Ньютона. https://uk.wikipedia.org/wiki/Метод_Ньютона*

*105. Національна система електронного ЕЦП. Технічні специфікації форматів представлення базових об'єктів. www.stc.gov.ua/document/68848/DOC1474.PDF*

*106. ПЛИС, САПР и средства отладки фирмы Xilinx. КТЦ "Инлайн Груп". Июнь 2018. http://plis.ru/custom/announcements/2018_03_30/table_selection_guide_2018.pdf*

*107. Энциклопедия кибернетики. Главная редакция украинской советской*

*энциклопедии. Киев – 1975.*

*108. S. J. Aboud, "An Efficient Method for Finding Square Root," International Journal of Statistics, ISSN:2051-8285, vol. 37, no. 1, pp. 1103-1106, 2013.*

*109. Gora Adj and Francisco Rodrıguez-Henrıquez, "Square root computation over even extension fields," IEEE Transactions on Computers, vol. 63, no. 11, pp. 2829 - 2841, Nov 2014*

*110. M. Bednara, Michael Daldrup, Joachim von zur Gathen, J¨urgenTeich, Jamshid Shokrollahi, "Reconfigurable Implementation of Elliptic Curve Crypto Algorithms," in 9th Reconfigurable Architecture Workshop (RAW 2002), 2002.*

*111. E. R. Berlekamp, H. Rumsey, And G. Solomon, "On the Solution of Algebraic Equations over Finite Fields, Information and Control 1O, 553-564, Jet Propulsion Laboralory, Pasadena, California 91103,USA, June 1967.*

*112. Hannes Bernien, Sylvain Schwartz, Alexander Keesling, Harry Levine, Ahmed Omran, Hannes Pichler, Soonwon Choi, Alexander S. Zibrov, Manuel Endres, Markus Greiner, Vladan Vuletić & Mikhail D. Lukin. Probing many-body dynamics on a 51-atom quantum simulator. Nature volume551, pages 579–584 (30 November 2017). Macmillan Publishers Limited, part of Springer Nature. All rights reserved.*

*113. Vishwas Bhargava, Gábor Ivanyos, Rajat Mittal, Nitin Saxena, "Irreducibility and r-th root finding over finite fields," Cornell University , USA, 2017. arXiv preprint arXiv:1702.00558*

*114. Bernstein, D. Post-quantum cryptography / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p.*

*115. T. Carmely. Using finite state machines to design software. http://www.embedded.com/design/testissue/216200597?pgno=1 (03/30/09 EDT).*

*116. Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. CRYPTO 2016: Advances in Cryptology – CRYPTO 2016. pp 572-601*

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

*118. Jean-Pierre Deschamps. José Luis Imaña. Gustavo Sutter. Hardware Implementation of Finite-Field Arithmetic. McGraw Hill, March 2009. ISBN: 978-0-0715-4581-5*

*119. Vassyl Dimitrov, Kimmo Järvinen, "Another Look at Inversions over Binary Fields" in Computer Arithmetic (ARITH), 2013 21st IEEE Symposium, Austin, TX, USA, 2013.*

*120. M. Ernst, M. Jung, F. Madlener, S. Huss, and R. Blümel. A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography over GF($2^n$). (2002). www.vlsi.informatik.tu-darmstadt.de/staff/madlener/publications/iss_tud_ches02.pdf*

*121. R. Gallant, R. Lambert, S. Vanstone "Improving the parallelized Pollard lambda search on binary anomalous curves" to appear in Mathematics of Computation.*

*122. Grover, L. K. A fast quantum mechanics algorithm for database search [Electronic resource] / L. K. Grover // CERN Document Server. – Available at: http://cds.cern.ch/record/304210/files/9605043.pdf*

*123. Guild, H.H . Fully iterative fast array for binary multiplication and addition. Electronics Letters, Volume 5, Issue 12, 12 June 1969, page 263.*

*124. Hae Young Kim, Jung Youl Park, Jung Hee Cheon, Je Hong Park1, Jae Heon Kim, and Sang Geun Hahn. Fast Elliptic Curve Point Counting using Gaussian Normal Basis. Lecture Notes In Computer Science; Vol. 2369. Proceedings of the 5th International Symposium on Algorithmic Number Theory. Pages: 292 – 307. Year of Publication: 2002.*

*ISBN:3-540-43863-7. http://portal.acm.org/citation.cfm?id=750068*

*125. Hankerson Darrel R. Guide to elliptic curve cryptography / Darrel Hankerson, Alfred J. Menezes, Scott Vanstone. (c) 2004 Springer-Verlag New York, Inc.*

*126. M.A. Hasan, A.G. Wassal. VLSI Algorithms, Architectures, and Implementation of a Versatile GF($2^m$) Processor. IEEE TRANSACTIONS ON COMPUTERS, VOL. 49, NO. 10, OCTOBER 2000, pp. 1064-1073.*

*127. V. Hlukhov. Open Systems Model for Specialized Computer Systems.*

*Матеріали конференції CADSM2005. Славське, 2005.*

*128. Valerii Hlukhov. Implementing Quantum Fourier Transform in a Digital Quantum Coprocessor. Advances in Cyber-Physical Systems. Volume 4. Number 1. Lviv Polytechnic National University. 2019. pp. 6 - 13.*

*129. Valerii Hlukhov, Bohdan Havano. FPGA-based Digital Quantum Coprocessor. Advances in Cyber-Physical Systems. Volume 3. Number 2. Lviv Polytechnic National University. 2018. pp. 12 - 31.*

*130. Valerii Hlukhov, Bohdan Havano. Principles of Digital Quantum Coprocessor Based on a FPGA, which Operates under the Control of a Classical Computer. Advanced Computer Information Technologies Acit 2019. June 5 - 7, 2019. International Conference. Ceske Budejovice, Czech Republic. Conference Proceedings, pp. 191 – 194.*

*131. Atef Ibrahim, Hamed Elsimary, Fayez Gebali. New Systolic Array Architecture For Finite Field Division. IEICE Electronics Express. Https://Doi.Org/10.1587/Elex.15.20180255 Issn-L: 1349-2543. P. 20180255 . 2018*

*132. Itoh, T., Teechai, O., and Tsujii, S. "A Fast Algorithm for Computing Multiplicative Inverses in GF(2t) Using Normal Bases," J. Society for Electronic Communications (Japan) 44 (1986), pp. 31-36.*

*133. Jungnickel D. Finite fields: Structure and arifmetics. Wissenschfttsverlag, 1995.*

*134. R. V. Kamala (MS by Research). VLSI Implementation of High Speed Galois Field Modular inversion resistive to Side-Channel Attacks. Center for VLSI and Embedded System Technologies, International Institute of Information Technology, Hyderabad. iiit_kamala_present[1].ppt. http://www.getgyan.com/show/2167/VLSI_Implementation_of_High_Speed_Galois_Field_Modular_Inversion_Resistive_to_Side_Channel_Attacks*

*135. N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203–209.*

*136. Koblitz, N. A riddle wrapped in an enigma [Electronic resource] / N. Koblitz, A. J. Menezes // ePrint Archive. – 2016. – P. 1–21. – Available at:*

*http://eprint.iacr.org/2015/1018.pdf*

*137. Sudha Ellison Mathe, Lakshmi Boppana. Bit-Parallel Systolic Multiplier Over GF($2^m$). Https://Doi.Org/10.1049/Iet-Cds.2017.0426. Source: Volume 12, Issue 4, July 2018, P. 315 – 325. © The Institution Of Engineering And Technology Received 10/10/2017, Accepted 03/01/2018, Revised 19/12/2017, Published 05/01/2018*

*138. Oleksandr Martynyuk, Hanna Stepovaya, Bui Van Thiong, Dmitry Martynyuk. Behavioral model of resource diagnostics of network components. Міжнародна науково-практична конференція «Електротехнічні та комп'ютерні системи: Теорія та практика» ЕЛТЕКС – 2018. м. Одеса, 29 травня – 1 червня 2018 року*

*139. Maurer, Peter M. Primitive Polynomials for the Field GF(3). Dept. of Computer Science, Baylor University, Waco, Texas 76798. https://baylor-ir.tdl.org/handle/2104/8793 29.08.2019*

*140. N. Mentens, Sıddıka Berna O¨ rs, Bart Preneel. An FPGA Implementation of an Elliptic Curve Processor over GF($2^m$). GLSVLSI'04, April 26–28, 2004, Boston, Massachusetts, USA. Copyright 2004 ACM 1-58113-853-9/04/0004. https://www.cosic.esat.kuleuven.be/publications/article-29.pdf*

*141. A. Menezes, P van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.*

*142. V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.*

*143. Amin Monfared, Hayssam El-Razouk, Arash Reyhani-Masoleh, "A New Multiplicative Inverse Architecture in Normal Basis Using Novel Concurrent Serial Squaring and Multiplication" in IEE: Computer Arithmetic (ARITH), 2017 IEEE 24th Symposium, London, UK, 2017.*

*144. Moody, D. Post-Quntum Cryptography: NIST's Plan for the Future [Electronic resource] / D. Moody // The Seventh International Conference on Post-Quntum Cryptography. – 2016. – Available at: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf*

*145. Mullin R.C., Onyszchuk I.M., Vanstone S.A., Wilson R.M. Optimal normal bases in GF($p^n$). Discrete Applied Mathematics (1988/89), vol.22, 149-161.*

*146. Petrus Mursanto, Aulia Roza Albareta. Circular Shift Squarer For Efficiency Improvement Of Normal Basis Galois Field Inverter. Https://Doi.Org/10.1109/Icacsis.2018.8618150 Published In: IEEE 2018 International Conference On Advanced Computer Science And Information Systems (Icacsis) Date Of Conference: 27-28 Oct. 2018 Date Added To Ieee Xplore: 21 January 2019.*

*147. Petrus Mursanto, R. Dimas Nugroho. New Polynomial Based Bit-Level Serial GF($2^m$) Multiplier For RS(15,11) 4-Bit Codec Optimization. Published In: Ieee 2018 International Workshop On Big Data And Information Security (IWBIS) Https://Doi.Org/10.1109/Iwbis.2018.8471694 Date Of Conference: 12-13 May 2018*

*148. Parham Hosseinzadeh Namin, Crystal Roma, Roberto Muscedere, Majid Ahmadi. Efficient VLSI Implementation Of A Sequential Finite Field Multiplier Using Reordered Normal Basis In Domino Logic. Https://Doi.Org/10.1109/Tvlsi.2018.2851958 Published In: Ieee Transactions On Very Large Scale Integration (VLSI) Systems (Volume: 26, Issue: 11, Nov. 2018) Page(S): 2542 – 2552 Date Of Publication: 09 August 2018.*

*149. J. Omura and J. Massey. Computational method and apparatus for finite field arithmetic. U.S. Patent Number 4,587,627, May 1986.*

*150. Patterson D., Hennessy J. Computer Architecture. A quantitative Approach. 6th Edition. - Morgan Kaufmann Publishers, Inc., San Francisco, California, 2017. – 936 p.*

*151. Steffen Peter, Peter Langendorfer, Krzysztof Piotrowski. Public key cryptography empowered smart dust is affordable. International Journal of Sensor Networks. 2008 Vol. 4. No. 1/2, pp. 130 - 143.*

*152. Rahma, M. Galois Fields Elements Processing Units for Cryptographic Data Protection in Cyber-Physical Systems / V. Hlukhov, I. Zholubak, A. Kostyk, M. Rahma / Advances in Cyber-Physical Systems, Вид-во Національного університету Львівська політехніка. - Volume 2, Number 2, 2017. – pp. 47- 53.*

*153. Rahma, M. FPGA cores for fast multiplicative inverse calculation in Galois Fields / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak.*

*Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 27(103), с. 227-233*

*154. Rahma, Mohammed Kadhim. Galois Field Operational unit For Elliptic Curve Cryptography Digital Signature. V Міжнародний молодіжний науковий форум "Litteris et Artibus". 26–28 листопада, 2015. Україна, Львів. Pp. 66-71.*

*155. Rahma, Mohammed Kadhim. Time complexity of multipliers for Galois fields / Mohammed Kadhim Rahma, Valeriy S.Hlukhov / INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24-26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52-53*

*156. Rahma, M. Computing Square Roots and Solve Equations of ECC over Galois Fields /M. Rahma, V. Hlukhov / International Youth Science Forum "Litteris Et Artibus", November 23-25, 2017, Lviv, Ukraine, pp. 437-440*

*157. Rahma, Mohammed Kadhim. Automation System for Configuration of Cryptographic Data Protection Unit Model / Ivan Zholubak, Mohammed Kadhim Rahma and Valeriy Hlukhov / Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv, pp. 669-679.*

*158. Rahma, Mohammed. Devices for Multiplicative Inverse Calculation in Binary Galois Fields / Valeriy Hlukhov, Mohammed Rahma and Ivan Zholubak. / Proceedings of 9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT'2018. Kyiv, May 24-27, pp. 275-278.*

*159. Rahma, Mohammed. Hardware components for post-quantum elliptic curves cryptography / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. / Proceedings of International Conference "Advanced Computer Information Technologies", June 1-3, 2018 in Ceske Budejovice, Czech Republic, pp. 236-239.*

*160. Bahram Rashidi; Reza Rezaeian Farashahi; Sayed Masoud Sayedi, "High-performance and high-speed implementation of polynomial basis Itoh–Tsujii inversion algorithm over GF(2^m)" The Institution of Engineering and Technology, vol. 11, no. 2, p. 66 – 77, 2017.*

*161. M. Repka, "Computing pth roots in extended finite fields of prime characteristic p ≥ 2," The Institution of Engineering and Technology, vol. 52, no. 9, p. 718 – 719, 2016.*

*162. Arash Reyhani-Masoleh, Hayssam El-Razouk, Amin Monfared. New Multiplicative Inverse Architectures Using Gaussian Normal Basis. Https://Doi.Org/10.1109/Tc.2018.2859941 Published In: Ieee Transactions On Computers (Early Access ) Page(S): 1 – 1. Date Of Publication: 26 July 2018.*

*163. Robinson Steve. Safe and secure: data encryption for embedded systems. EDN Europe, 01 Jun 2008, pp.24-33.*

*164. F. Rodríguez-Henríquez, N.A. Saqib, A. Díaz-Pèrez, Çetin Kaya Koç. Cryptographic Algorithms on Reconfigurable Hardware. Springer. © 2006 Springer Science.*

*165. P. Rohatgi. Technology: Can mil systems be hacked? On dangerous ground: The rise and fall of military systems power. Military Embedded Systems. June 2010, volume 6, number 4, pp. 28-30.*

*166. P. Rohatgi. Protecting FPGAs from simple and differential power analysis. Embedded control Europe. September 2010. pp. 25 – 28.*

*167. K. H and P. Rosen, HANDBOOK OF DISCRETE MATHEMATICS and ITS APPLICATIONS, Boca Raton, FL 33487-2742: Taylor & Francis Group, LLC, 2013*

*168. R. Rozario. Hardware authentication secures design IP and end-user experience. Embedded Computing Design, May 2010, pp. 17 – 20.*

*169. Savaş, E. & Koç, Ç.K. J, "Montgomery inversion," Journal of Cryptographic Engineering, vol. 10, no. 1, pp.1-10, 2017.*

*170. Chang, Seunghwan; Kim, Bihtnara; Lee, Hyang-Sook, "Polynomial representations for n-th roots in finite fields". Journal of the Korean Mathematical Society, vol. 52, no. 1, pp. 209-224, 2015.*

*171. Qiliang Shao, Zhenji Hu, Shaik Nazeem Basha, Zhiping Zhang, Zhiqiang Wu. "Low Complexity Implementation Of Unified Systolic Multipliers For NIST Pentanomials And Trinomials Over GF($2^m$)" Https://Doi.Org/10.1109/Tcsi.2018.2795380 Published In: Ieee Transactions On*

*Circuits And Systems I: Regular Papers, Page(S): 2455 – 2465, Volume: 65,Issue: 8, Aug. 2018*

*172. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor //SIAM J. Comput. – 1997. – 26 (5). –P. 1484–1509.*

*173. M. Smerdon. Security Solutions Using Spartan-3 Generation FPGAs. © 2007-2008 Xilinx, Inc. WP266 (v1.1) April 22, 2008.*

*174. Stein, J. "Computational problems associated with Racah algebra", Journal of Computational Physics, 1 (3): 397–405, doi:10.1016/0021-9991(67)90047-2, ISSN 0021-9991. 1967*

*175. D. Stewart. Migrating software into hardware. EDN Europe, Issue 12/2008, p. 48.*

*176. Trichina E., Korkishko T., Lee K.-H.: Small size, low power, side channel immune AES co-processor: Design and synthesis resultys. In Proc. Of Forth Conf. on Advanced Encryption Standard (AES 2005), Volume 3373 of Lecture Notes in Computer Science, pp.113-127, Springer-Verlag, 2006.*

*177. Ellappan Venugopal, Tadesse Hailu. Fpga Based Architecture Of Elliptic Curve Scalar Multiplication For IOT. Https://Doi.Org/10.1109/Icedss.2018.8544305 Published In: IEEE 2018 Conference On Emerging Devices And Smart Systems (ICEDSS) Date Of Conference: 2-3 March 2018.*

*178. R. Wilson. Electronic-system-level design: is there fire beneath the smoke? EDN Europe magazine. October 2008, pp.25-31.*

*179. Haibo Yi, Zhe Nie. High-Speed Hardware Architecture For Implementations Of Multivariate Signature Generations On FPGAs. Https://Doi.Org/10.1186/S13638-018-1117-2; Https: //Link.Springer.Com/Content/Pdf/10.1186%2fs13638-018-1117-2.Pdf, Yi And Nie Eurasip Journal On Wireless Communications And Networking (2018) 2018:93*

*180. Valeriy Zadiraka, Yaroslav Nykolaychuk, Stepan Ivasiev. The theory of factorization multidigit numbers. The Experience of Designing and Application of*

*CAD Systems in Microelectronics. 24-27 Feb. 2015. Lviv, Ukraine. Conference Proceedings. Pp. 221 – 225*

*181. Zhou, Fan. Study Of Extended Euclidean And Itoh-Tsujii Algorithms In GF($2^m$) Using Polynomial Bases. Uri: Https://Dspace.Library.Uvic.Ca//Handle/1828/9023 Date: 2018-01-30*

*182. Zode P., Deshmukh R.B., Samad A., "Fast Architecture of Modular Inversion Using Itoh-Tsujii Algorithm," Springer, Singapore, vol. 711, no. VDAT 2017, pp. 48-55, 2017*

*183. AMERICAN NATIONAL STANDARD X9.62-1998. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm.*

*184. Applying Multicore and Virtualization to Industrial and SafetyRelated Applications. http://www.embedded-know-how.com. Printed in USA 0209/SI/S2/PDF. Copyright © 2009 Intel Corporation.*

*185. BSI TR-02102-1. Technical Guideline – Cryptographic Algorithms and Key Lengths. Version: 2018-02. Federal Office for Information Security 2017.*

*186. Certicom ECC Challenge. http://www.certicom.com/download/aid-111/cert_ecc_challenge.pdf. Copyright 2008 Certicom Corp.*

*187. Data Protection IP Cores. http://intron-innovations.com/?p=crypto_ip*

*188. ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY. Editor-in-chief Henk C.A. van Tilborg. Eindhoven University of Technology. The Netherlands. © 2005 Springer Science+Business Media, Inc.*

*189. FIPS PUB 186-2. Federal InformationProcessing Standards Publication 186-2. 2000 January 27. DIGITAL SIGNATURE STANDARD (DSS).*

*190. FPGA-to-ASIC Conversion.*

*http://www.onsemi.ru.com/PowerSolutions/content.do?id=16788*

*191. IEEE 1363-2000. Standard Specifications for Public-Key Cryptography. Copyright © 2000 IEEE. All rights reserved.*

*192. ISO/IEC 14888-3:1998. Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms.*

*193. KippsDeSanto A&D and Government Services 2018 M&A Survey. https://kippsdesanto.com › uploads › 2018/07*

*194. Keys length recommendations. © 2018 BlueKrypt (http://www.bluekrypt.com) - Version 31.0 - June 10 2018.*

*195. Maple User Manual. Copyright © Maplesoft, a division of Waterloo Maple Inc. 2017*

*196. National Institute for Standards and Technology, "Recommended Elliptic Curves for Federal Government Use", July 1999, <http://csrc.nist.gov/encryption/NISTReCur.pdf>*

*197. Password cracking. https://en.wikipedia.org/wiki/Password_cracking*

*198. Review Acer Aspire 4830TG Notebook. https://www.notebookcheck.net/Review-Acer-Aspire-4830TG-Notebook.53433.0.html*

*199. SEC 2: Recommended Elliptic Curve Domain Parameters. Certicom Research. September 20, 2000. Version 1.0*

*200. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop [Text] / M. Mosca, G. Lenhart, M. Pecen (Eds.) // E-proceedings of "1st Quantum-Safe-Crypto Workshop". – Sophia Antipolis, 2013. – 289 p. – Available at: https://docbox.etsi.org/ Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf*

*201. Spartan-3 FPGA Family: Introduction and Ordering Information. DS099 (v3.1) June 27, 2013. © Copyright 2003–2013 Xilinx, Inc.*

*202. Spartan-6 Family Overview. DS160 (v2.0) October 25, 2011. © 2009–2011 Xilinx, Inc.*

*203. UG116 (v10.8.1). Device Reliability Report. May 3, 2018*

*204. XAPP371 (v1.0) CoolRunner-II CPLD Galois Field GF($2^m$) Multiplier. September 26, 2003.*

*205. Xilinx Intellectual Property (IP) cores address requirements for DSP, Embedded, and Connectivity designs. http://www.xilinx.com/products/intellectual-property/index.htm*

*206. http://ru.wikipedia.org/wiki/IP-cores. 01:33, 19 травня 2019.*

*207. www.rsasecurity.com/rsalabs/challenges.*

*208. ETSI GR QSC 001 V1.1.1 (2016-07). Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. GROUP REPORT. © European Telecommunications Standards Institute 2016. All rights reserved.*

*209. Why Use Cryptography? © 2016 Certicom Corp. © 2016 QNX Software Systems Limited. https://www.certicom.com/content/dam/certicom/images/pdfs/why-cryptography.pdf*

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
Національного університету
"Львівська політехніка"
_____ Чухрай Н.І.
"09" 04 2019 р.

**АКТ**

про використання результатів дисертації випускника аспірантури 2018 р. Рахма Мохаммед Кадім Рахма «Моделі та методи побудови операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих», представленої на здобуття наукового ступеня кандидата технічних наук, при виконанні держбюджетної науково-дослідної роботи ДБ/КІБЕР кафедри електронних обчислювальних машин Національного університету «Львівська політехніка»

Комісія у складі: голови – начальника науково-дослідної частини (НДЧ), к.т.н., доцента Жук Л.В., завідувача відділу науково-організаційного супроводу наукових досліджень, к.т.н. Лазько Г.В., завідувача кафедри електронних обчислювальних машин, д.т.н., професора Мельника А.О., та заступника начальника планово-фінансового відділу Чулой Т.М. цим актом підтверджують, що результати кандидатської дисертації випускника аспірантури 2018 р. Рахма Мохаммед Кадім Рахма «Моделі та методи побудови операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих» використано при виконанні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446).

В результаті досліджень, виконаних Рахма Мохаммед Кадім Рахма:

створено і апробовано технологічний засіб (генератор ядер) для проектування операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих;

створено і перевірено уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі таких, які маскують роботу засобів КЗІ;

визначено найкращі для використання розширені поля Галуа.

Голова комісії
начальник НДЧ,
к.т.н., доцент _____ Жук Л.В.

Члени комісії:
завідувач відділу науково-організаційного
супроводу наукових досліджень, к.т.н. _____ Лазько Г.В.
зав. каф. ЕОМ, д.т.н., професор _____ Мельник А.О.
заступник начальника
планово-фінансового відділу _____ Чулой Т.М.

# ДОДАТОК Б. АКТ ВПРОВАДЖЕННЯ (AL-NABAA NETWORK SOLUTION L.L.C.)

www.alnabaa.iq

شركة النبع لحلول الشبكات ذ.م.م.

Re: Usage of Research Results from the Ph.D. Thesis (Models and design methods of operational units for processing of GF elements) of Mr. Mohammed Kadhim Rahma..

The main results of the thesis (Models and design methods of operational units for processing of GF elements) of Mr. Mohammed Kadhim Rahma that is applied to get a Ph.D. degree is used within our line of business at Al Nabaa Network solutions .

The main effects and benefits of using these results helped us enhance our work through :

1. Security provided by Digital Signatures
2. High performance for the algorithm used
3. Efficiency and functionality of the multiplier
4. Efficiency and functionality of the multiplicative inverse
5. Difficulty to hacking the data and information
6. High efficiency of concurrent Error detection

AL-NABAA Co. Network Solutions LLC شركة النبع لحلول الشبكات المحدودة

Executive Manager
Nazar Lateef

العراق . بغداد . شارع الصناعة. مقابل الجامعة التكنولوجية
مبنى النبع . ص.ب ٣٥٠٥٥ هـ : ٧١٩٤٣٣٦ ف : ٧١٧٠١٧٤
موبايل ٠٧٧٠٥٣٨٥٠٣٦

IRAQ,Baghdad,Al-Sina'a Street,AL-NABAA Building
P.: 35055 T.:+964(0)1 7194336 F.: +964(0)1 7170174
M.: +964(0)770 538 5036
E.: solutions@al-nabaa.net W.: www.alnabaa.iq

AL-NABAA Network Solution L.L.C.

**ЗАТВЕРДЖУЮ**

Проректор з науково-педагогічної роботи

Національного університету

"Львівська політехніка"

д.т.н, доц. _____ О. Р. Давидчак

"08" 2019 р.

**АКТ**

**про використання результатів дисертаційного дослідження випускника**

аспірантури кафедри електронних обчислювальних машин

Рахма Мохаммед Кадім Рахма

на тему: «Моделі та методи побудови операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих» за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти»

Комісія у складі: голови – завідувача кафедри електронних обчислювальних машин (ЕОМ), д.т.н, професора Мельника А. О., членів комісії: к.т.н., доц. Березко Л. О., к.т.н., доц. Ваврука Є. Я. цим Актом засвідчує, що результати дисертаційного дослідження Рахма Мохаммед Кадім Рахма на тему: «Моделі та методи побудови операційних вузлів для полів Галуа, що використовуються при криптографічному захисті інформації на основі еліптичних кривих» використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій автоматики та метрології (ІКТА) Національного університету «Львівська політехніка» при підготовці і проведенні курсу лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проектування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна

інженерія», спеціалізації «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»), що підтверджено цим Актом).

Голова комісії

Зав. каф. ЕОМ, д.т.н., професор _____ Мельник А. О.

Члени комісії

Доц. каф. ЕОМ, к.т.н., доцент _____ Березко Л. О.

Доц. каф. ЕОМ, к.т.н., доцент _____ Ваврук Є. Я.

«29» 08 2019 р.

# ДОДАТОК Г. АТАКИ НА ІНФОРМАЦІЙНІ ЗАСОБИ

Класифікують такі типи атак на засоби захисту інформації:

простих атак на основі споживаної потужності [188, *side-channel analysis*];

диференційних атак на основі споживаної потужності;

простих атак на основі електромагнітного випромінювання [188, *electromagnetic attack*];

диференційних атак на основі електромагнітного випромінювання;

аналізу теплових режимів;

аналізу даних, що опрацюовуються;

аналізу звукових режимів;

аналізу деталей проєкту;

аналізу часових характеристик;

аналізу реакції на помилки.

Метою простих атак є визначення секретного ключа, метою диференційних атак є визначення даних, що опрацювується.

Рис. Г.1 [166] ілюструє просту атаку - визначення секретного ключа в методі RSA шляхом аналізу споживаної потужності при виконанні множення (M) і піднесення до квадрату (S). Рис. Г.2 [165] ілюструє диференційну атаку – зміну споживаної потужності при використанні правильно підібраного ключа (верхній графік) і неправильно підібраного ключа (нижній графік). Рис. Г.3 [125] містить приклад вимірювання споживаною потужності під час виконання операцій над точками ЕК: *S* – операція додавання точок, *D* – операція подвоєння точок, одиниці на осях - умовні. Відома послідовність операцій дозволяє визначити розряди ключа.

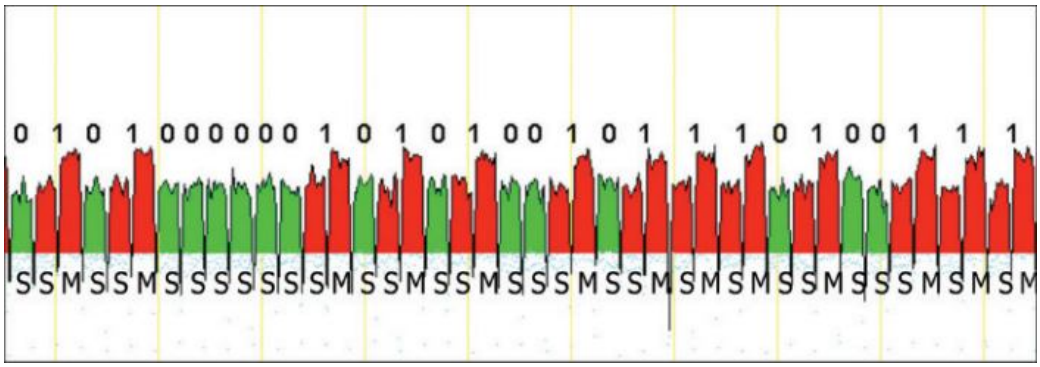



Рис. Г.1. Проста атака

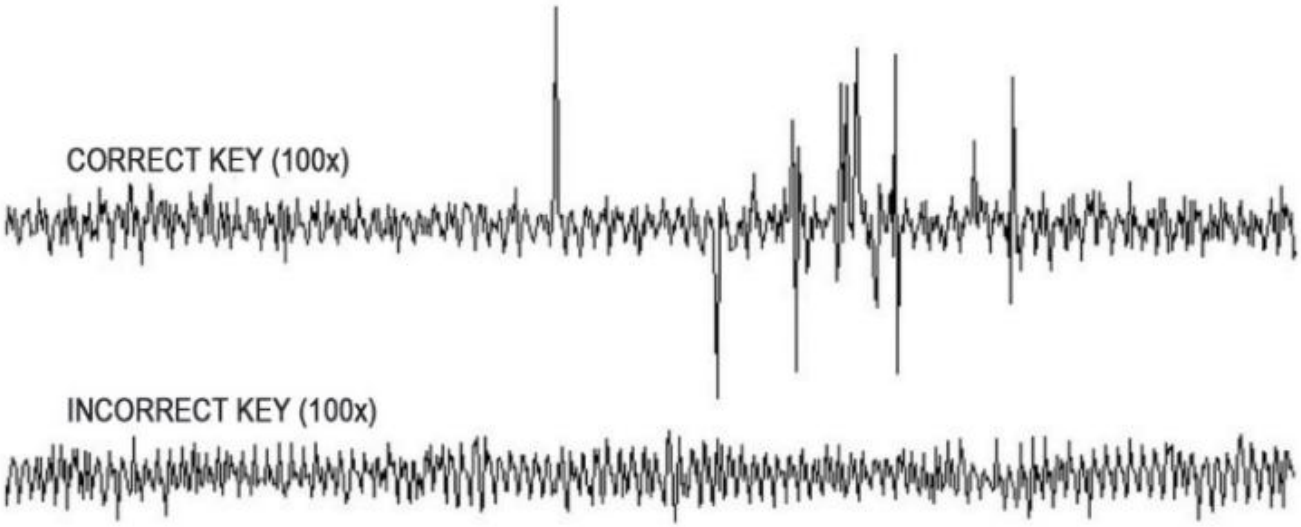



Рис. Г.2. Диференційна атака

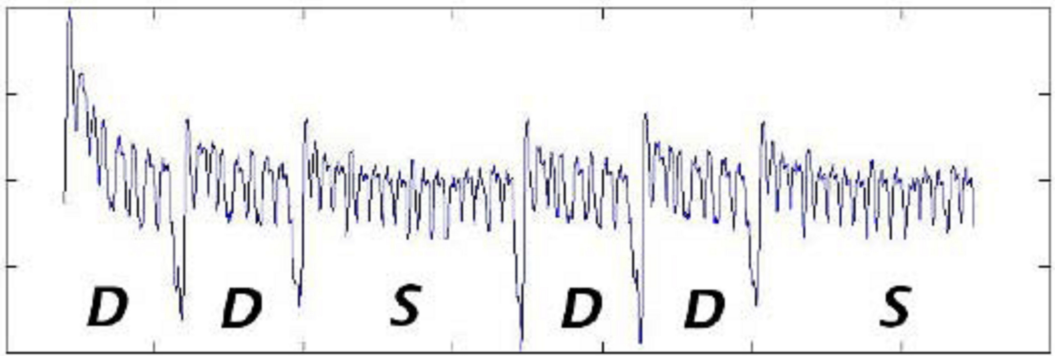



Рис. Г.3. Зміна споживаної потужності

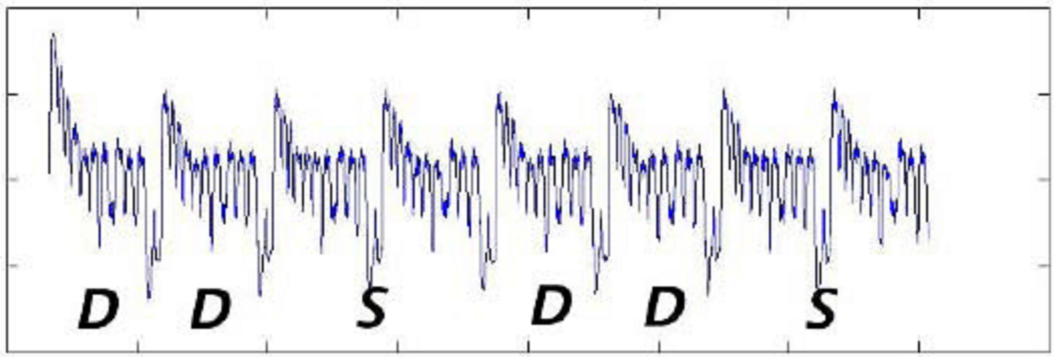



Рис. Г.4. Зміна споживаної потужності вирівняних за часом операціях

# ДОДАТОК Д. ВЕРИФІКАЦІЇ ПОВІДОМЛЕННЯ НА БАЗІ ЕЦП

Для верифікації повідомлення *M* (користувач *A* - користувачу *B*) необхідно:

відправник (користувач *A*) повинен внести в *M* підпис *SIG*{$k_A$, *M*, ідентифікатор *B*}, що містить додаткову інформацію, залежну від *M* , від одержувача повідомлення *B* і відомої тільки відправнику закритої інформації $k_A$;

для попередження повторного використання застарілих повідомлень процедура додавання підпису повинна залежати від часу;

користувач *B* повинен мати можливість упевнитися, що *SIG*{$k_A$, *M*, ідентифікатор *B*} - є правильний підпис *M* користувачем *A*.

Підпис повідомлення - певний спосіб перетворення *M* шляхом відповідного перетворення. Елементом $k_A$ є ключ перетворення, який належить кінцевій множині ключів *K*. Вичерпне перевіряння всіх ключів, повинне привести до визначення ключа $k_A$ зловмисником. Коли говорять, що скласти правильний підпис без ключа неможливо, мають на увазі, що визначення *SIG*{$k_A$, *M*, ідентифікатор *B*} без $k_A$ з обчислювальної точки зору еквівалентно пошуку ключа.

Хоча одержувач інформації не може скласти правильний підпис, він повинен уміти засвідчувати його достовірність. Встановлення достовірності підпису - це процес, за допомогою якого кожна сторона встановлює достовірність іншої. Обов'язковою умовою цього процесу є збереження таємниці. Для того, щоб в системі опрацювання даних одержувач міг встановити достовірність відправника, необхідне виконання наступних умов.

Відправник (користувач *A*) повинен забезпечити одержувача (користувача *B*) інформацією *AUTH*{$k_A$, *M*, ідентифікатор *B*}, яка його засвідчує і яка залежить від секретної інформації $k_A$, відомої тільки користувачу *A*.

Необхідно, щоб інформацію *AUTH*{$k_A$, ідентифікатор *B*}, яка засвідчує користувача *A*, користувачу *B* можна було дати тільки за наявності ключа $k_A$.

Користувач *B* повинен мати в своєму розпорядженні процедуру перевіряння того, що *AUTH*{$k_A$, ідентифікатор *B*} дійсно підтверджує особу користувача *A*.

Для попередження використання попередньої перевіреної на достовірність інформації процес встановлення достовірності повинен мати залежність від часу.

# ДОДАТОК Е. ВИКОРИСТАННЯ ЕЛІПТИЧНИХ КРИВИХ

## Е.1. Історичний огляд

У 1985-86 р. В. Міллер [142] і Н. Кобліц [135] запропонували використовувати ЕК для криптографічних цілей. У 1998 році *ISO* [192], в 1999-м *ANSI* [183], а в 2000 році *IEEE* [78] і *NIST* [189] прийняли новий стандарт для ЕЦП *ECDSA* (*Elliptic Curve Digital Signature Algorithm*), заснований на використанні ЕК. У 2002 році в Україні був прийнятий аналогічний стандарт [93]. З 1 січня 2004 року в Україні набрав чинності закон про ЕЦП [102], що надає право фізичним і юридичним особам використовувати ЕЦП для підтвердження матеріалів і документів, поданих в електронній формі.

## Е.2. Еліптичні криві над полем $GF(2^m)$

Нехай $m > 3$ - ціле число. Нехай a, $b \in GF(2^m)$, $b \neq 0$. ЕК $E$ над полем $GF(2^m)$ називається множина розв'язків $(x, y)$ рівняння $y^2 + xy = x^3 + ax^2 + b$ над полем $GF(2^m)$ разом з додатковою точкою $\infty$, званою точкою в нескінченності.

Кількість точок $\#E$ на кривій $E$ також визначається теоремою Хассе:

$q + 1 - 2\sqrt{q} \le \# E \le q + 1 + 2\sqrt{q}$, де $q = 2^m$. Більш того, $\#E$ парне.

Операція додавання на $E$ в цьому випадку задається наступними правилами:

$\infty + \infty = \infty$; $\forall (x, y) \in E, (x, y) + \infty = (x, y)$; $\forall (x, y) \in E, (x, y) + (x, x + y) = \infty$;

$\forall (x_1, y_1) \in E, (x_2, y_2) \in E, x_1 \neq x_2, (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, де

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \lambda = \frac{y_1 + y_2}{x_1 + x_2}.$$

$\forall (x_1, y_1) \in E, x_1 \neq 0, (x_1, y_1) + (x_1, y_1) = (x_2, y_2)$, де $x_2 = \lambda^2 + \lambda + a$, $y_2 = x_1^2 + (\lambda + 1)x_2, \lambda = x_1 + \frac{y_1}{x_1}$.

В цьому випадку множина точок ЕК $E$ із заданою таким чином операцією також утворює абельову групу.

Користуючись операцією додавання точок на кривій, можна природним чином визначити операцію множення точки $P \in E$ на довільне ціле число $n$: $nP = P + P + \ldots + P$, де операція додавання виконується $n$ раз.

**Псевдовипадкові криві.** Для кожного поля $GF(2^m)$, може бути знайдена

псевдовипадкова крива, яка має вигляд [189] $E: y^2 + x\,y = x^3 + x^2 + b$, $b \in GF(2^m)$, $b \neq 0$. Крива позначається *B-m*. Такі криві використані у стандарті [93].

**Криві Кобліца.** Для кожного поля може бути знайдена крива Кобліца (або анормальна двійкова крива), яка має вигляд [189] $E: y^2 + x\,y = x^3 + ax^2 + 1$, $a \in GF(2^m)$, $a \in \{0,1\}$. Крива позначається *K-m (m* – розширення поля).

Е.3. Операції над точками еліптичних кривих

Е.3.1. Додавання точок еліптичної кривої

Припустимо, що ми знайшли на ЕК $y^2 = x^3 + ax + b$ (Рис. Е.1) дві раціональні точки $P(x,y)$ і $Q(x,y)$.

Проведемо пряму $PQ$ і обчислимо координат третьої точки перетину прямої з нашою кривою. Ці координати задовольняють системі рівнянь

$$\begin{cases} y^2 = x^3 + ax + b, \\ (y - y_P)(x_Q - x_P) = (x - x_P)(y_Q - y_P). \end{cases}$$

Якщо $x_P \neq x_Q$ і $y_P \neq y_Q$, то приходимо до кубічного рівняння для $y$ з раціональними коефіцієнтами. Оскільки два корені цього рівняння раціональні (вони рівні $y_P$ та $y_Q$,), а сума усіх трьох коренів - раціональне число (за теоремою Вієта), то, третій корінь теж раціональний. Отже, по двох раціональних точках, що лежать на ЕК, можна побудувати третю раціональну точку. Ще одна раціональна точка виходить з побудованої точки симетрією щодо осі $Ox$. Ця симетрична точка називається сумою точок $P$ і $Q$ і позначається $P+Q$. Введена операція додавання точок ЕК має властивості операції додавання чисел, а саме:

а) комутативність (для будь-яких точок $P$ і $Q$ ЕК $P + Q = Q + P$);

б) наявність нуля (такої точки О, що $P+O=O+P=P$ для будь-якої точки Р ЕК);

в) наявність для будь-якої точки $P$ ЕК протилежної точки $-P$ ($P+(-P)=(-P)+P=O$);

г) асоціативність (для будь-яких точок $P$, $Q$ і $R$ ЕК $(P + Q) + R = P + (Q + R)$.

Е.4. Сингулярні та суперсингулярні криві

Кількість точок еліптичної кривої Е (включаючи нескінчену віддалену точку ОЕ) називають порядком (або потужністю) кривої Е та позначають #Е.

Еліптичну криву E, над полем GF(p), яка має порядок #E = p+1, називають суперсингулярною. Еліптичну криву E, над полем GF(p), яка має порядок #E = p, називають аномальною.

Еліптичну криву $E$, над полем $GF(2^m)$, яка має порядок $\#E = 2^m+1 - t$, називають суперсингулярною, якщо $t$ - парне.

Загалом, еліптичну криву $E$, над полем $GF(p^m)$, яка має порядок $\#E = 2^p+1 - t$, називають суперсингулярною, якщо $p$ ділить $t$. Суперсингулярні та аномальні криві у криптографічних прикладеннях не використовуються [98].

Якщо $b = 0$, то така крива називається сингулярною кривою і не є еліптичною кривою.

Прикладами суперсингулярних еліптичних кривих є криві вигляду $y^2 = x^3 + ax$ над полем $GF(p)$, коли $p = -1(mod4)$ та $y^2 = x^3 + b$ над полем $GF(p)$, коли $p = -1(mod3)$ [50].

### E.5. Множення точок еліптичних кривих. Кратні точки [78]

Важливу роль в алгоритмах підпису з використанням ЕК грають «кратні» точки. Точка $Q$ називається точкою кратності $k$, якщо для деякої точки $P$ $k$ раз виконано рівність: $P = Q + Q + Q + \ldots + Q = kQ$. Випадок $P = Q + Q = 2Q$ ілюструється Рис. E.1. Дана операція називається подвоєнням точок ЕК. Точки більшої кратності знаходяться додаванням точок меншої кратності. Якщо для деякої точки $P$ існує таке число $k$, що $kP = 0$, це число називають порядком точки $P$.

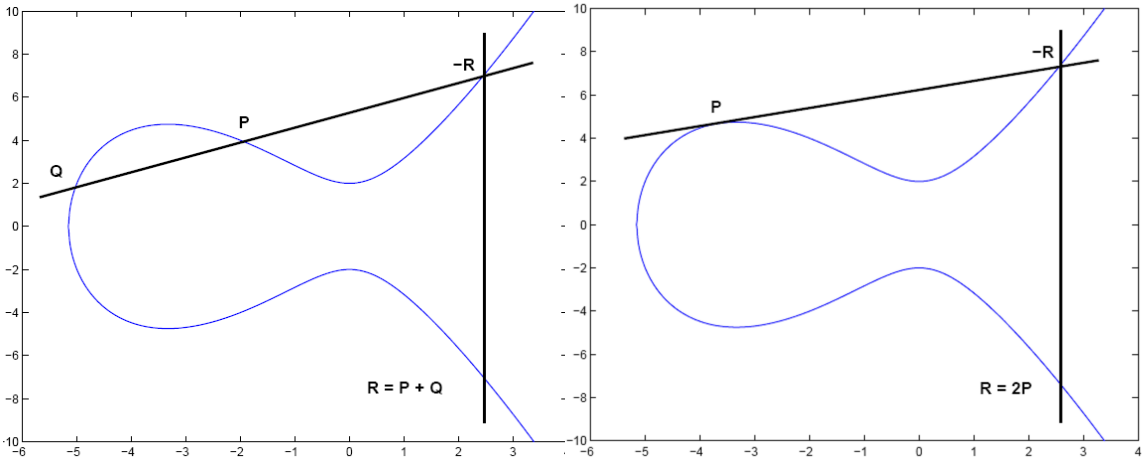



Рис. E.1. Додавання та подвоєння точок еліптичної кривої

Кратні точки ЕК є аналогом степенів чисел в простому полі. Завдання обчислення кратності точки еквівалентне завданню обчислення дискретного

логарифма. Але обчислення кратності має більшу складність, на цьому і заснована надійність ЕЦП. Саме тому при побудові алгоритмів підпису в групі точок ЕК виявилося можливим обійтися коротшими ключами при забезпеченні більшої стійкості.

Е.6. Протокол на основі ЕК

Для встановлення захищеного зв'язку два користувачі *A* і *B* спільно вибирають ЕК *E* і точку *P* на ній. Потім кожний з користувачів вибирає своє секретне ціле число, відповідно *a* і *b*. Користувач *A* обчислює добуток *aP*, а користувач *B* - *bP*. Далі вони обмінюються обчисленими значеннями. При цьому параметри самої кривої, координати точки на ній і значення добутків є відкритими. Потім користувач *A* помножує отримане від *B* значення на *a*, а користувач *B* помножує отримане їм значення на *b*. Через властивості операції множення на число $abP = baP$. Таким чином, обидва користувачі отримають загальне секретне значення (*abP*), яке вони можуть використовувати для отримання ключа шифрування. Зловмиснику для відновлення ключа потрібно вирішити складне з обчислювальної точки зору завдання визначення *a* і *b* по відомих *E*, *P*, *aP* і *bP*.

# ДОДАТОК Ж. МАТЕМАТИЧНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

Під алгеброю розуміється наука про множини об'єктів, між якими встановлені так звані алгебраїчні операції [63]. Алгебраїчна операція це правило, яке довільному впорядкованому набору елементів даної множини ставить в однозначну відповідність суворо визначений елемент цієї ж множини. Можливий варіант, коли вказана відповідність регламентується не для будь-яких наборів елементів, така операція називається частковою. Далі подібні операції не розглядаються. Найбільше значення мають бінарні операції, які кожній впорядкованій парі елементів даної множини ставлять у відповідність третій елемент цієї множини. Бінарна операція на множині $K$ - це відображення $K \times K \to K$, де декартовий добуток $K \times K$ - це множина всіх впорядкованих пар елементів із заданої множини $K$.

**Група.** Множина $K$ із заданою на ньому бінарною операцією * називається групою (позначення: $G$ = <К;*>, якщо операція * наділена наступними властивостями (задовольняє список наступних аксіом) [63]:

1. Замкнутість - будь-якій парі ($\alpha$, $\beta$) елементів з множини $K$ ставиться в однозначну відповідність третій елемент $\gamma \in K$, можливо, він збігається з одним з початкових елементів $\alpha$ або $\beta$ (система <К;*> з цією властивістю називається групоїдом).

2. Асоціативність, тобто $(\alpha\beta)\gamma = \alpha(\beta\gamma) = \alpha\beta\gamma$ для $\{\alpha, \beta, \gamma\} \in K$ (система з властивостями пп. 1 і 2 - напівгрупа).

3. Наявність “нейтрального” елементу е, такого, що $e\alpha = \alpha e = \alpha$ для $\alpha \in K$ (система з властивостями пп. 1…3 - моноїд).

4. Існування для кожного елементу $\alpha \in K$ оберненого $x \in K$ такого, що $x\alpha = \alpha x = e$.

5. Група називається комутативною або абельовою на честь видатного норвезького математика Н. Абеля (*N.H. Abel*, 1802-1829), якщо групова операція * є комутативною. Таким чином, аксіоми пп. 1…4 доповнюються ще однією.

6. Комутативність, тобто $\alpha\beta = \beta\alpha$. Замість символу * бінарній операції прийнято використовувати знак суми «+» (адитивний запис) або добутку «·» (мульти-

плікативний запис), причому крапку як символ операції множення між буквами-співмножниками допустимо опускати.

7. При адитивному записі нейтральний елемент позначається 0, тобто $0+\alpha = \alpha+0 = \alpha$, а обернений до $\alpha$ елемент називається протилежним і позначається $(-\alpha)$, тобто $\alpha + (-\alpha) = 0$.

8. При мультиплікативному записі нейтральний і обернений до $\alpha$ елементи позначаються відповідно 1 і $\alpha^{-1}$, тобто $\alpha\cdot 1 = 1\cdot\alpha = \alpha$ і $\alpha\cdot\alpha^{-1} = \alpha^{-1}\cdot\alpha = 1$.

**Поле.** Розглянемо алгебру $<K; +,\cdot >$, тобто множини з парою бінарних операцій (адитивної і мультиплікативної). Першу назвемо “додаванням”, а другу - “множенням”. Якщо ж можливо змішування знаків «+» і «·» із звичайними арифметичними операціями, то значення символів пояснюється окремо.

Поле - це множина не менше ніж з двох елементів, над якими задана пара бінарних операцій, званих “додаванням” і “множенням” і які володіють тією властивістю, що для них існують обернені операції: віднімання і ділення (окрім ділення на нуль), причому множення дистрибутивне щодо додавання.

Отже, поле це алгебра $<K;+,\cdot,-,:>$.

**Поля Галуа.** Скінчена алгебра поля Э. Галуа (*E.Galois*, 1811-1832) містить скінчену кількість елементів $K=\{ 0, 1, 2,\ldots, i\}$. Проте, не для будь-якого числа елементів можна підібрати такі операції, що система $<K; +,\cdot >$ є полем. Скінчені поля, що позначаються $GF(p^r)$, існують лише порядку (з числом елементів) $p^r$, де $p$ - просте число (характеристика поля), $r$ - натуральне число (розмірність поля). При $r = 1$ маємо просте поле $GF(p)$ з розглянутими вище модульними операціями додавання і множення. Якщо ж $p$ - складене число, то система $<K;+,\cdot>$, де додавання і множення - модульні операції, полем не є: ця система утворює так зване кільце, в якому ділення навіть на ненульовий елемент можливо не завжди.

У будь-якому полі множина $K$ всіх елементів утворює за операцією додавання циклічну (адитивну) групу; аналогічно, множина $K_0$ ненульових елементів утворює за операцією множення циклічну (мультиплікативну) групу. Поле $GF(p^r)$ називається розширення поля $GF(p)$.

*Таблиця Ж. 1*

## Математичні пакети

| Назва пакета (розширення пакету) | Фірма | Можливість роботи у $GF(p^m)$ | Примітки |
|---|---|---|---|
| MathCAD 14.0 | Parametric Technology Corporation | p =2,<br>$m \leq 600$,<br>поліноміальний базис | |
| Mathlab R2008b (Communications Toolbox) | The Math-Works, Inc. | p – просте число, $m \leq 16$,<br>поліноміальний базис | |
| Mathematica 7 | Wolfram Research, Inc. | p – просте число, m – обмежено тільки можливостями комп'ютера і часом (перевірено до m=500, коли m наближається до 500 починається нестабільна робота програми, зависання), поліноміальний базис | |
| Maple 14 | Waterloo Maple Inc. | p – просте число, m – обмежено тільки часом (перевірено до m=4000), поліноміальний базис | |

# ДОДАТОК З. ОПТИМАЛЬНІ І ГАУСІВСЬКІ НОРМАЛЬНІ БАЗИСИ

Для оптимізації часу множення або схемної реалізації множення в нормальних базисах використовують оптимальні або близькі до них Гаусові нормальні базиси. Відповідно до [145] складністю $C_B$ довільного нормального базису $B = \{ x, x^q, x^{q^2}, ..., x^{q^{n-1}} \}$ називається число ненульових елементів в матриці $T$, $i$-ий рядок якої є вектор $xx^{q^{n-1}}$ коефіцієнтів поля $GF(2^n)$ щодо базису $B$, тобто $xx^{q^i} = \sum_{j=0}^{n-1} t_{i,j} x^{q^j}$ .

Це визначення мотивується наступним алгоритмом множення в нормальному базисі $B$ (алгоритмом *Massey-Omura* [149], див., наприклад [133]): нехай $\xi = \sum_{i=0}^{n-1} x_i x^{q^i}$ , $\zeta = \sum_{j=0}^{n-1} y_i x^{q^j}$ довільні елементи поля $GF(q^n)$, розкладені по нормальному базису $B$, тоді їх добуток можна обчислити за формулою:

$$\pi = \xi\zeta = \sum_{i,j=0}^{n-1} x_i y_j x^{q^i + q^j} = \sum_{i,j=0}^{n-1} x_i y_j x^{(q^{i-j}+1)q^j} ,$$

де різниця $i - j$ обчислюється за модулем $n$, а оскільки

$$x^{\left(q^{i-j}+1\right)q^j} = \left( x^{q^{i-j}+1} \right)^{q^j} = \left( \sum_{k=0}^{n-1} t_{i-j,k} x^{q^k} \right)^{q^j} = \sum_{k=0}^{n-1} t_{i-j,k} x^{q^{k+j}} = \sum_{m=0}^{n-1} t_{i-j,m-j} x^{q^m} ,$$

де різниця $m - j$ і сума $k + j$ теж обчислюються за модулем $n$, то $\pi = \sum_{m=0}^{n-1} p_m x^{q^m}$ ,

де $p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_i$ - деяка білінійна форма над полем $GF(q)$.

Оскільки при піднесенні елементів $\xi$, $\zeta$ д о степеню $q$ відбувається циклічний зсув змінних в кожному з векторів $x_i$, $i = 1, ..., n$ та $y_i$, $i = 1, \ldots, n$ на одну позицію управо, а $\pi^q = \xi^q \zeta^q$, то координати елементу $\pi^q$ обчислюються за формулами $P_i = p_i(S(x), S(y))$. Але при піднесенні елементу $p$ до ступеня $q$ відбувається такий ж циклічний зсув координат, тобто, координата $p_i$ переходить в координату $p_{i+1 \bmod n}$

означає $p_{i+1 \bmod n}(x, y) = p_i(S(x),S(y)), i = 0, ..., n-1$ звідки витікає, що $P_{i\text{-}kmodn}(x,y) = p_i(S^k(x),S^k(y)), i = 0, ..., n\text{-}1$, тобто, решта всіх форм виходить з форми $p_0$ за формулою $p_{m \bmod n}(x,y) = p_0(S^{n-m}(x),S^{n-m}(y)), k = 1, ..., n\text{-}1$, де $S^{n-m}$ - операція циклічного зсуву координат вектора вправо на $n - m$ позицій, або, що рівносильно, вліво на $m$ позицій. Цей зсув можна явно визначити формулою

$$S^{n-m}(x_0, \ldots, x_{n-1}) = (x_m, \ldots, x_{n-1}, x_0, \ldots, x_{m-1}) = (x_{i+m \bmod n}, i = 0, \ldots, n-1).$$

Визначивши матрицю $A$ рівністю $a_{i,j} = t_{i-j,-j}$, де *i-j ma –j* обчислюються за модулем $n$, помічаємо, що попередню формулу можна переписати у вигляді

$$p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_i = p_0\left(S^{n-m}(x), S^{n-m}(y)\right),$$

де $p_0(x,y) = A(x,y) = \sum_{i,j=0}^{n-1} a_{i,j} x_i y_j$.

На відміну від матриці $T$ матриця $A$ симетрична, але число її ненульових елементів, а також їх сума такі ж, як і у матриці $T$. Для обчислення білінійної форми $A(x,y)$ досить виконати $2C_B + n - 1$ додавань і множень в полі $GF(q)$. Якщо нехтувати часом виконання циклічних зсувів, то складність виконання множення над нормальним базисом поля $GF(q^n)$ оцінюється зверху як $n(2C_B + n - 1)$ операцій в полі $GF(q)$, що видно з наступної формули:

$$\xi\zeta = A(\xi,\zeta) + A\left(\xi^{q^{n-1}}, \zeta^{q^{n-1}}\right)x^q + A\left(\xi^{q^{n-2}}, \zeta^{q^{n-2}}\right)x^{q^2} + \ldots + A\left(\xi^q, \zeta^q\right)x^{q^{n-1}}.$$

Таким чином, складність множення залежить тільки від кількості ненульових елементів $C_B$ в матриці $A$.

# ДОДАТОК И. МЕТОДИ ОБЧИСЛЕННЯ ОБЕРНЕНОГО ЕЛЕМЕНТА

У поліноміальному базисі для знаходження оберненого елемента використовується узагальнений алгоритм Евкліда обчислення найбільшого спільного дільника (НСД) двох многочленів $f(t)$ та $c(t)$ [191]. Цей алгоритм виражає НСД $d(t)$ як $d(t)=a(t)f(t)+b(t)c(t)$, де $a(t)$ і $b(t)$ - деякі многочлени, що обчислюються при виконанні узагальненого алгоритму Евкліда. Цей алгоритм діє наступним чином [93]:

*1. Приймають $a(t)=1$, $d(t)=f(t)$, $u(t)=0$, $v(t)=c(t)$.*

*2. Якщо $v(t)=0$, то приймають $b(t)=\dfrac{d(t)+f(t)a(t)}{c(t)}$, та закінчують виконання алгоритму.*

*3. За допомогою ділення з залишком обчислюють $d(t)=q(t)v(t)+r(t)$, далі обчислюють $w(t)=a(t)+u(t)q(t)$, $a(t)=u(t)$, $d(t)=v(t)$, $u(t)=w(t)$, $v(t)=r(t)$ та переходять до кроку 2.*

Якщо як $f(t)$ взяти примітивний многочлен поля, а замість $c(t)$ – многочлен, що зображає елемент поля, то $d(t)$ є одиничний многочлен і наведене вище співвідношення за модулем примітивного многочлена перетворюється на співвідношення $b(t)c(t)=1 \ mod \ f(t)$, тобто многочлен $b(t)$ зображує елемент, обернений до $c(t)$. Складність цього алгоритму дорівнює $O(m^2)$ [141]. Недоліком методу є залежність часу обчислень від значення операнда.

Інший подібний метод на основі модифікованого алгоритму Штайна [174] використовує систолічний масив операційних елементів [131].

**Методи обчислення оберненого елемента у нормальному базисі. Метод Іто-Тічей-Цудзії.** Для обчислення оберненого елемента в оптимальному нормальному базисі [191] використовується формула: $x^{-1}=x^{2^m-2}=x^{2(2^{m-1}-1)}$, $x\neq 0$. Для обчислення правої частини існує ефективний алгоритм [132]: нехай $m_r$, …, $m_0$ – двійковий розклад цілого числа $m$-1. Тоді обчислення оберненого елемента виконують так:

*1. $b \leftarrow x$; $k \leftarrow 1$.*
*2. Для $i$ від $r$-1 до 0 обчислюють:*
*2.1. $c \leftarrow b$;*
*2.2. для $j$ від 1 до $k$ обчислюють $c \leftarrow c^2$;*
*2.3. $b \leftarrow bc$;*

*2.4. $k \leftarrow 2k$;*

*2.5. якщо $m_i=1$, то $b \leftarrow b^2 x$ та $k \leftarrow k+1$.*

*3. $x^{-1}=b^2$.*

Даний метод характеризується часом обчислення, який не залежить від коду операнда. Відомі апаратні рішення [162], які реалізують цей метод.

Відомі також алгоритми [119], які базуються на використанні подвійних базових і потрійних базових представлень, є більш економічними, ніж алгоритм [132]. Окрім того, що в них виконується менше множення, вони дозволяють більш ефективно обчислювати квадрати, а в деяких випадках вимагають менше тимчасових змінних, але у стандартах вони не згадуються. У роботі [182] акцентується увага на паралельній архітектурі для алгоритму [132] шляхом введення $2^3$ його блоків, що може також служити для маскування роботи пристрою. У роботі [143] розглядається алгоритм знаходження оберненого елемента, який базується на класичному алгоритмі [132], що використовує взаємопов'язані обчислення двох простих множень і піднесення до квадрату на цифровому рівні.

У [169] було запропоновано два ефективні алгоритми Монгомері з постійним часом виконання, які корисні як контрзаходи проти атак бічними каналами. В роботі [160] представлено реалізації в ПЛІС у поліноміальному базисі алгоритму [132] над $GF(2^m)$, побудованим незвідними тричленами та п'ятичленами. Запропоновані вузли розробляються з одним помножувачем поля та k квадраторами (виконують піднесення до степені $2^k$), де k - невелике натуральне число. В [156] було представлено квадратори, корисні для реалізації алгоритму [132].

# ДОДАТОК К. ПРИКЛАД ОБЧИСЛЕННЯ ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА МЕТОДОМ НЬЮТОНА-РАФСОНА

**Example** for *m*=5: $a^{-1} = a^{i-1-2^m} = a^{i-31}$. **T**he inverse operation will be only in half part from $a^{16}$ to $a^{30}$.

$a^{-1} = p_3$; where $p_4 = \sqrt[2]{a \otimes p_3} = 1$:

| $a^{i}$ | $a^{i-31}$ | $a^{i}$ | $a^{i-31}$ | **Operation** |
|---|---|---|---|---|
| $a^{0}$ | $a^{-31}$ | $a^{16}$ | $a^{-15}$ | $p_0 = \sqrt[2]{a} = a^{16}$ |
| $a^{1}$ | $a^{-30}$ | $a^{17}$ | $a^{-14}$ | |
| $a^{2}$ | $a^{-29}$ | $a^{18}$ | $a^{-13}$ | |
| $a^{3}$ | $a^{-28}$ | $a^{19}$ | $a^{-12}$ | |
| $a^{4}$ | $a^{-27}$ | $a^{20}$ | $a^{-11}$ | |
| $a^{5}$ | $a^{-26}$ | $a^{21}$ | $a^{-10}$ | |
| $a^{6}$ | $a^{-25}$ | $a^{22}$ | $a^{-9}$ | |
| $a^{7}$ | $a^{-24}$ | $a^{23}$ | $a^{-8}$ | |
| $a^{8}$ | $a^{-23}$ | $a^{24}$ | $a^{-7}$ | $p_1 = \sqrt[2]{a \otimes p_0} = a^{-7}$ |
| $a^{9}$ | $a^{-22}$ | $a^{25}$ | $a^{-6}$ | |
| $a^{10}$ | $a^{-21}$ | $a^{26}$ | $a^{-5}$ | |
| $a^{11}$ | $a^{-20}$ | $a^{27}$ | $a^{-4}$ | |
| $a^{12}$ | $a^{-19}$ | $a^{28}$ | $a^{-3}$ | $p_2 = \sqrt[2]{a \otimes p_1} = a^{-3}$ |
| $a^{13}$ | $a^{-18}$ | $a^{29}$ | $a^{-2}$ | |
| $a^{14}$ | $a^{-17}$ | $a^{30}$ | $a^{-1}$ | $p_3 = \sqrt[2]{a \otimes p_2} = a^{-1}$ |
| $a^{15}$ | $a^{-16}$ | $a^{31}$ | $a^{0}$ | |

# ДОДАТОК Л. ОГЛЯД МЕТОДІВ ЗНАХОДЖЕННЯ КОРЕНІВ У СКІНЧЕНИХ ПОЛЯХ

У статті [113] була обговорена гіпотеза значно слабша, ніж узагальнена гіпотеза Рімана, для отримання детерміністичного алгоритму для знаходження кореня степені r. Прямий метод обчислення кореня p-го степеня в будь-яких розширених кінцевих полях характеристики $p \geq 2$, що працюють з довільними незвідними поліномами наведено в роботі [161]. [170] узагальнює результати обчислення кореня степені n у скінчених полях з довільною характеристикою у поліноміальному базисі. У [109] наведено комплексне дослідження методів обчислення квадратних коренів у скінченних розширених полях та запропоновано два нові алгоритми для обчислення квадратних коренів у розширених полях з парними степенями полів. [108] розглядає деякі методи знаходження квадратних коренів, які потребують більш ніж одного піднесення до степеня в кінцевому полі.

## Л.1. Обчислення сліду

Нехай для $c_i \in \{0,1\}$, що представляється як $c = (c_{n-1},...,c_0)$, є метод обчислення слід $Tr(c)$, за визначенням сліду, який вимагає *m-1* піднесення до квадрату у полі і *m-1* операцій додавання у полі. Набагато більш ефективний метод використовує те, що трасування є лінійним [125], [167]: $Tr(c) = Tr(\sum_{i=0}^{n-1} c_i z^i) = \sum_{i=0}^{n-1} c_i (Tr(z)^i)$.

Оператор сліду має важливі властивості $Tr(y^2) = Tr(y)$ і $Tr(x+y) = Tr(x) + Tr(y)$ для всіх $x, y \in GF(2^n)$.

Значення $Tr(z)^i$ може бути попередньо обчислено, дозволяючи ефективно знаходити слід елемента, особливо якщо $Tr(z)^i = 0$ для більшості *i*. Наступні приклади показують обчислення слідів елементів у $GF(2^{163})$ з утворюючим многочленом $f(z) = z^{163} + z^7 + z^6 + z^3 + 1$. Прямий розрахунок показує, що $Tr(z)^i = 1$ якщо і тільки якщо $i \in \{0,157\}$. Як приклади, $Tr(z^{160} + z^{46}) = 0$, $Tr(z^{157} + z^{46}) = 1$ і $Tr(z^{157} + z^{46} + 1) = 0$.

## Л.2. Вдосконалений метод обчислення квадратних коренів

Основний метод обчислення квадратного кореня в $GF(2^n)$ ґрунтується на малій теоремі [125]: $c^{2^n} = c$. Тоді $\sqrt{c} = c^{2^{n-1}}$ у полі $GF(2^m)$, його можна порахувати за

допомогою $m-1$ піднесень до квадрату.

Більш ефективний метод отриманий з спостереження, що $\sqrt{c}$ можна виразити через квадратний корінь елемента z.

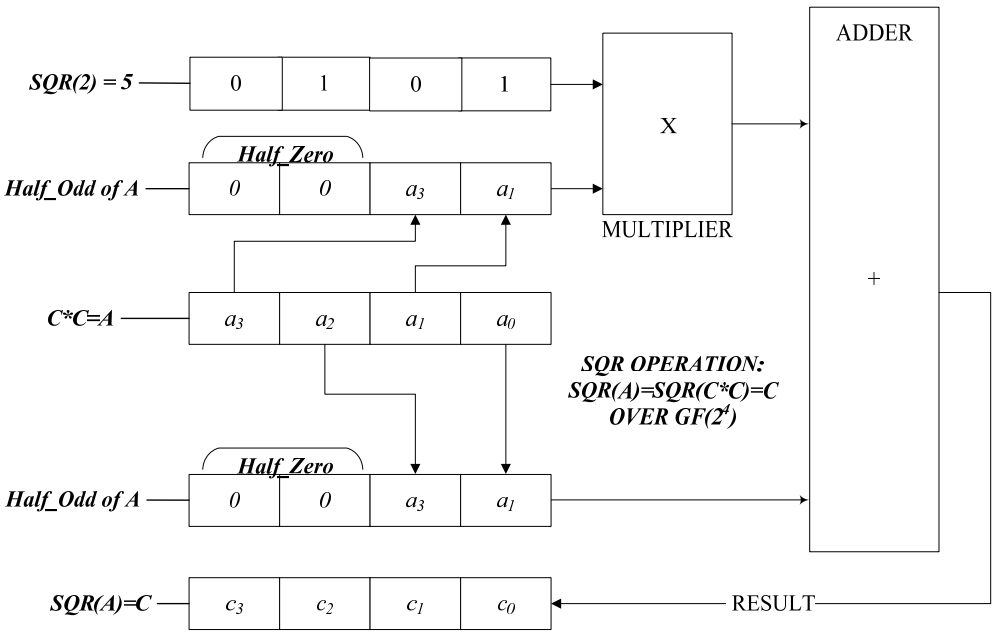
Нехай є поле $GF(2^n)$, $c_i \in \{0,1\}$. Оскільки квадрат є лінійною операцією у $GF(2^n)$, квадратний корінь операнда c може бути записаний як

$$\sqrt{c} = \left( \sum_{i=0}^{m-1} c_i z^i \right)^{2^{m-1}} = \sum_{i=0}^{m-1} c_i (z^{2^{m-1}})^i .$$

Розподіливши c на парні і непарні степені отримаємо

$$\sqrt{c} = \sum_{i=0}^{\frac{m-1}{2}} c_{2i} (z^{2^{m-1}})^{2i} + \sum_{i=0}^{\frac{m-3}{2}} c_{2i+1} (z^{2^{m-1}})^{2i+1} = \sum_{i=0}^{\frac{m-1}{2}} c_{2i} z^i + \sum_{i=0}^{\frac{m-3}{2}} c_{2i+1} z^{2^{m-1}} z^i$$
$$= \sum_{i_{even}} c_i z^{\frac{i}{2}} + \sqrt{z} \sum_{i_{odd}} c_i z^{\frac{i-1}{2}} .$$

Це показує ефективний метод для обчислення $\sqrt{c}$: вилучити два вектори половинної довжини $c_{even} = (c_{n-1}, ..., c_4, c_2, c_0)$ та $c_{odd} = (c_{n-2}, ..., c_5, c_3, c_1)$ з $c$ (вважаючи, що $m$ є непарним), виконати в полі множення $c_{odd}$ довжини $\left\lfloor \frac{m}{2} \right\rfloor$ з наперед обчисленим значенням $\sqrt{z}$, і, нарешті, додати ці результати разом (Рис. Л. 1). Приклад розрахунку квадратного кореня для $GF(2^4)$, $z=2$, $\sqrt{z} = 5 = 0101$, $f(z) = z+1$, $c=1110$, $\sqrt{c} = 1101$.




У випадку, коли утворюючий многочлен $f$ є тричленом, обчислення $\sqrt{c}$ може

бути ще більше прискорене оскільки формула для $\sqrt{z}$ може бути отримана безпосередньо з *f*.

Нехай $f(z) = z^m + z^k + 1$ є незвідним тричленом ступеня m, де m > 2 є простим. Розглянемо випадки, коли *k* непарний. Зауважте, що $1 \equiv z^m + z^k (mod\ f(z))$. Тоді, умноживши на z і беручи квадратний корінь, ми отримуємо $\sqrt{z} \equiv z^{m+\frac{1}{2}} + z^{k+\frac{1}{2}} (mod\ f(z))$.

Таким чином, добуток $\sqrt{z} \cdot c_{odd}$ вимагає двох операцій зсуву наліво та одного зведення за модулем. Тепер припустимо, що k парне. Зауважте, що $z^m \equiv z^k + 1 (mod\ f(z))$. Потім розділившись на $z^{m-1}$ і беручи квадратний корінь, ми отримуємо

$$\sqrt{z} \equiv z^{\frac{-(m-1)}{2}} (z^{\frac{k}{2}} + 1)(mod\ f(z)).$$

Для того, щоб обчислити $z^{-s}$ по модулю, де $s = \frac{m-1}{2}$, можна використовувати конгруентність $z^{-t} \equiv z^{k-t} + z^{m-t} (mod\ f(z))$ для $1 \le t \le k$, щоб записати $z^{-s}$ як сума декількох позитивних степенів z. Отже, добуток $\sqrt{z} \cdot c_{odd}$ може бути обчислено з декількома операціями зсуву ліворуч та одним модульним скороченням. Наприклад:

***Квадратні корені в*** $GF(2^{409})$**:** Утворюючий поле поліном за рекомендацією NIST є тричлен $f(z) = z^{409} + z^{87} + 1$. Потім нова формула для обчислення квадратного коріння з $c \in GF(2^{409})$ є $\sqrt{c} = (c_{evem} + z^{205} \cdot c_{odd} + z^{44} \cdot c_{odd}) mod\ f(z)$.

***Квадратні корені в*** $GF(2^{233})$**:** Утворюючий поле поліном за рекомендацією NIST є тричлен $f(z) = z^{233} + z^{74} + 1$. Оскільки *k*=74 є парним, ми маємо $\sqrt{z} = z^{-116} \cdot (z^{37} + 1) mod\ f(z)$, $z^{-74} \equiv (z^{159} + 1) mod\ f(z)$ та $z^{-42} \equiv (z^{32} + z^{191}) mod\ f(z)$. Тоді $z^{-116} \equiv (z^{32} + z^{117} + z^{191}) mod\ f(z)$. Отже, новий метод обчислення квадратного кореня з $c \in GF(2^{233})$ дає $\sqrt{c} = (c_{evem} + (z^{32} + z^{117} + z^{191})(z^{37} + 1) \cdot c_{odd}) mod\ f(z)$.

На додаток до вищесказаного, оскільки в будь-якому полі характеристик 2 ми маємо тотожність $(x+y)^2 = x^2 + y^2$ і, симетрично, $(x+y)^{1/2} = x^{1/2} + y^{1/2}$ квадратний корінь - це лінійна операція [111].

У базисі поля $GF(2^n)$, який записується як $u_1, u_2, ..., u_n$ ми можемо написати $c = \sum_{i=1}^{n} c_i u_i$, де $c \in GF(2)$. Через лінійність квадратного кореня ми маємо $\sqrt{c} = \sum_{i=1}^{n} c_i u_i^{1/2}$.

Звичайно $u_i^{1/2}$ також може бути представлено у тому ж базисі, як $u_i^{1/2} = \sum_{i=1}^{n} R_{i,j} u_j$, де $R_{i,j} \in GF(2)$. Тоді маємо $\sqrt{c} = \sum_{i=1}^{n} \sum_{j=1}^{n} c_i R_{i,j} u_j$, $\sqrt{c} = \sum_{j=1}^{n} (\sum_{i=1}^{n} c_i R_{i,j}) u_j$.

# ДОДАТОК М. VHDL-ОПИС ВУЗЛА HALF_EVEN_ODD

```
-----------------------------------------------------
--- VHDL-description  = Half_even_odd of c(x)
-----------------------------------------------------
library ieee;
use ieee.std_logic_1164.all;
use ieee.std_logic_arith.all;
use ieee.std_logic_unsigned.all;
use work.ECC.all;
ENTITY Half_even_odd IS

PORT(
 C: IN STD_LOGIC_VECTOR(M-1 DOWNTO 0);
 C_even,C_odd,square_root_2: OUT  STD_LOGIC_VECTOR(M-1 DOWNTO 0));
END Half_even_odd;

ARCHITECTURE Half_even_odd OF

Half_even_odd IS

SIGNAL h_even: STD_LOGIC_VECTOR (((M-((m mod 2)*1))/2)-(1-(m mod 2)) DOWNTO 0);
SIGNAL h_odd : STD_LOGIC_VECTOR (((M-((m mod 2)*3))/2)-(1-(m mod 2)) DOWNTO 0);
SIGNAL even_0: STD_LOGIC_VECTOR (((M-((m mod 2)*3))/2)-(1-(m mod 2)) DOWNTO 0):=(others => '0');
SIGNAL odd_0 : STD_LOGIC_VECTOR (((M-((m mod 2)*1))/2)-(1-(m mod 2)) DOWNTO 0):=(others => '0');
signal mult_done: STD_LOGIC;

begin

half_even:FOR i IN 0 TO ((M-((m mod 2)*1))/2)-(1-(m mod 2))
            GENERATE h_even(i)<=c(2*i);
            end GENERATE;

half_odd : FOR i IN 0 TO ((M-((m mod 2)*3))/2)-(1-(m mod 2))
            GENERATE h_odd(i)<=c(2*i+1);
            end GENERATE;

            c_odd  <= odd_0 & h_odd;
            c_even <= even_0 & h_even;

END Half_even_odd;
```

# ДОДАТОК Н. РЕКОМЕНДАЦІЇ ЩОДО ДОВЖИНИ КЛЮЧІВ

*Таблиця Н. 1*

**Рекомендації щодо довжини ключа**

| Метод, рік видання | Рік | Довжина ключа |
|---|---|---|
| Lenstra/Verheul , 2000 | 2012 | 149 |
| Lenstra Updated , 2004 | 2012 | 152 |
| Ecrypt II , 2011 | 2011-2014 | 160 |
| NIST , 2011 | 2011-2030 | 224 |
| FNISA, 2010 | 2010-2020 | 200 |
| BSA (signatures only), 2011 | 2011-2015 | 224 |

*Таблиця Н. 2*

**Рекомендовані довжини ключів**

| Date | Minimum of Strength | Symmetric Algorithms | Factoring Modulus | Discrete Logarithm Key | Discrete Logarithm Group | Elliptic Curve | Hash (A) | Hash (B) |
|---|---|---|---|---|---|---|---|---|
| (Legacy) | 80 | 2TDEA* | 1024 | 160 | 1024 | 160 | SHA-1** | |
| 2016 - 2030 | 112 | 3TDEA | 2048 | 224 | 2048 | 224 | SHA-224 SHA-512/224 SHA3-224 | |
| 2016 - 2030 & beyond | 128 | AES-128 | 3072 | 256 | 3072 | 256 | SHA-256 SHA-512/256 SHA3-256 | SHA-1 |
| 2016 - 2030 & beyond | 192 | AES-192 | 7680 | 384 | 7680 | 384 | SHA-384 SHA3-384 | SHA-224 SHA-512/224 |
| 2016 - 2030 & beyond | 256 | AES-256 | 15360 | 512 | 15360 | 512 | SHA-512 SHA3-512 | SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512 |

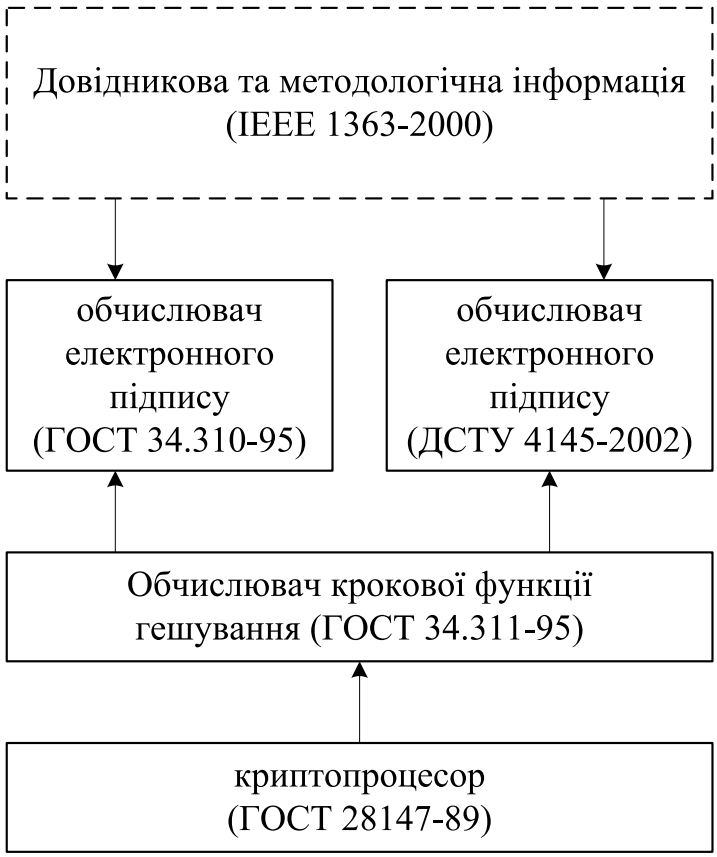
*Таблиця Н. 3*

**Стійкість засобів криптографічного захисту інформації**

| $log_2(R)$ | ECDLP | Factorisation / DLP in $\mathbb{F}_p^*$ |
|---|---|---|
| 60 | 120 | 700 |
| 70 | 140 | 1000 |
| 100 | 200 | 1900 |
| 128 | 256 | 3200 |
| 192 | 384 | 7900 |
| 256 | 512 | 15500 |

# ДОДАТОК О. НАЦІОНАЛЬНІ СТАНДАРТИ, ЩО ВИКОРИСТОВУЮТЬ ЕЛІПТИЧНІ КРИВІ

**Національні стандарти для ЕЦП.** Загальні параметри ЕЦП визначає [105]. У теперішній час на Україні діють стандарти на ЕЦП [89] та [93], останній містить посилання на стандарти [91] та [90] (замість яких зараз можна користуватися стандартами [100] та [101] відповідно) і разом із стандартами [98, 99] визначає алгоритми виконання операцій над точками ЕК та елементами поля Галуа $GF(2^p)$ (за винятком оптимального нормального базису, хоча і дає багато посилань на джерела, де можна знайти необхідні пояснення). Одним з цих джерел є [191]).




Діючі стандарти

**Стандарт електронного цифрового підпису ДСТУ 4145-2002.** Перелік основних математичних операцій стандарту містить таблиця.

Обчислення в групі точок еліптичної кривої.

Нехай $P = (x_P, y_P)$, $P \neq O$ і $Q = (xQ, yQ)$ $Q \neq O$, $P \neq Q$ — дві точки еліптичної кривої в афінних координатах. Сума цих точок $R = P + Q$ обчислюється за такими правилами.

$$x_R = \left(\frac{y_P + y_Q}{x_P + x_Q}\right)^2 + \frac{y_P + y_Q}{x_P + x_Q} + x_P + x_Q + A,$$

$$y_R = \left(\frac{y_P + y_Q}{x_P + y_Q}\right)(x_P + x_R) + x_R + y_P.$$

Якщо Q = -P, то R = O. Якщо Q ≠ -P, то координати (xR, yR ) точки R обчислюються за формулами:

$$x_R = x_P^2 + \frac{B}{x_P^2},$$

$$y_R = x_P^2 + \left(x_P + \frac{y_P}{x_P}\right)x_R + x_R.$$

*Таблиця*

**Основні операції за [93]**

| | Операції над точками ЕК | Операції над елементами основного поля $GF(2^m)$ | Операції над елементами поля $GF(2^m)$ |
|---|---|---|---|
| Визначення відкритого ключа | Q=-dP | | |
| Обчислення цифрового підпису | $R=eP=(x_R, y_R)=cT$ | $y = hF_e = hx_R$ | $s = (e+ dr) \bmod n$ |
| Перевіряння цифрового підпису | $R = sP + rQ = (x_R,y_R)=T_i+T_j=c_1T_1+c_2T_2$ | $y = hx_R$ | |

**Проблема інтероперабельності Національної системи електронного цифрового підпису**. До недоліків Національної системи ЕЦП відносять [57] її неінтероперабельність. Основна перешкода обумовлена орієнтацією на негармонізований національний стандарт [93], а не на міжнародні стандарти ЕЦП відповідно до гармонізованих діючих стандартів таких як ДСТУ *ISO/IEC* 14888:2015 [97].

# ДОДАТОК П. VHDL-ОПИСИ ЕЛЕМЕНТІВ ПОМНОЖУВАЧА

VHDL-опис модифікованої комірки Гілда Gn:

```
library IEEE;
use IEEE.STD_LOGIC_1164.all;
use IEEE.STD_LOGIC_unsigned.all;
use IEEE.STD_LOGIC_arith.all;

entity Gn is
        port(
                A : in STD_LOGIC_VECTOR(1 downto 0);
                B : in STD_LOGIC_VECTOR(1 downto 0);
                C : in STD_LOGIC_VECTOR(1 downto 0);
                S : out STD_LOGIC_VECTOR(1 downto 0)
            );
end Gn;

architecture Gn of Gn is
signal nc10     :std_logic;
signal ab00     :std_logic;
signal ab11     :std_logic;
signal ab01     :std_logic;
signal ab10     :std_logic;
signal na10     :std_logic;
signal nb10     :std_logic;
begin
                nc10 <= (not c(1)) and (not c(0));
                ab00 <= a(0) and b(0);
                ab11 <= a(1) and b(1);
                ab01 <= a(0) and b(1);
                ab10 <= a(1) and b(0);
                na10 <= (not a(1)) and (not a(0));
                nb10 <= (not b(1)) and (not b(0));
        s(0) <= (nc10 and ab00) or
                        (nc10 and ab11) or
                        (c(1) and ab01) or
                        (c(1) and ab10) or
                        (c(0) and na10) or
                        (c(0) and nb10);
        s(1) <= (nc10 and ab01) or
                        (nc10 and ab10) or
                        (c(0) and ab00) or
                        (c(0) and ab11) or
                        (c(1) and na10) or
                        (c(1) and nb10);
end Gn;
```

VHDL-опис вузла f помножувача:

```
library IEEE;
use IEEE.STD_LOGIC_1164.all;

entity f is
        port(
```

```
                A : in STD_LOGIC_VECTOR(1 downto 0);
                B : out STD_LOGIC_VECTOR(1 downto 0)
        );
end f;

architecture f of f is
begin
        process(A)
        begin
                B(0) <=         not A(1) and A(0);
                B(1) <=         not A(1) and not A(0);
        end process;
end f;
```

# ДОДАТОК Р. БЕЗПЕКА ІОТ

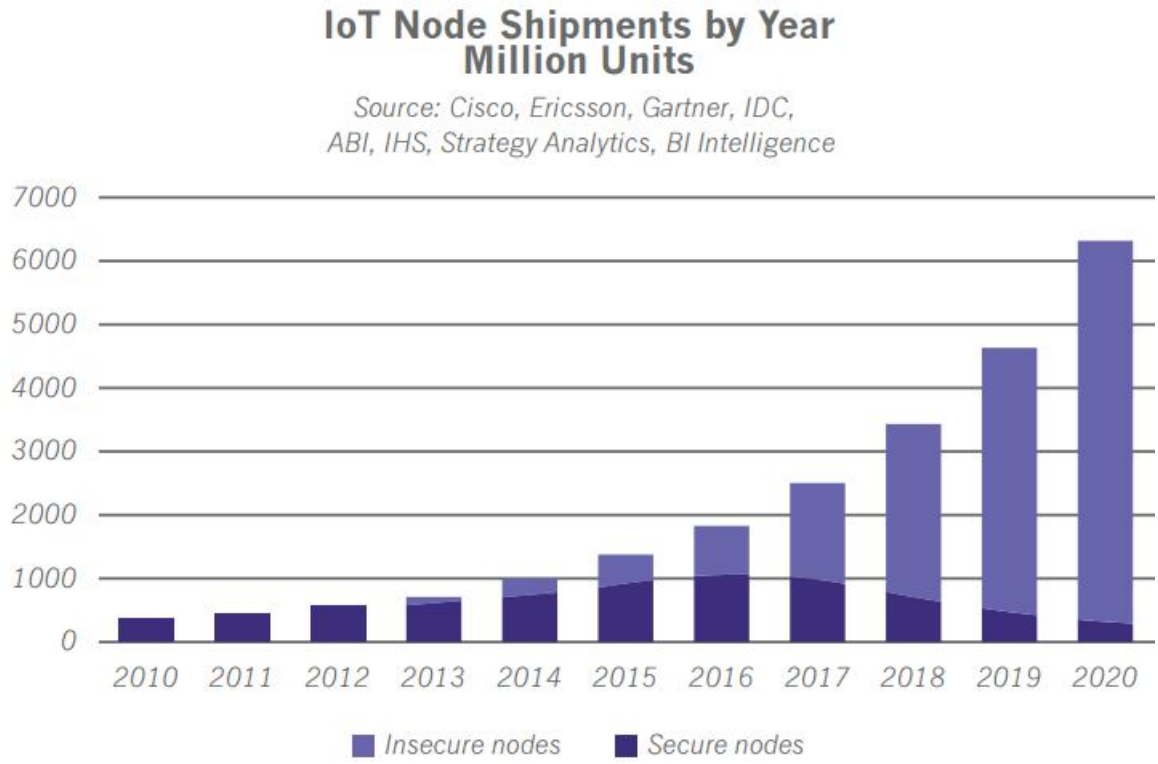



Рис. Р. 1. Захищене (темніше) і незахищене (світліше) обладнання

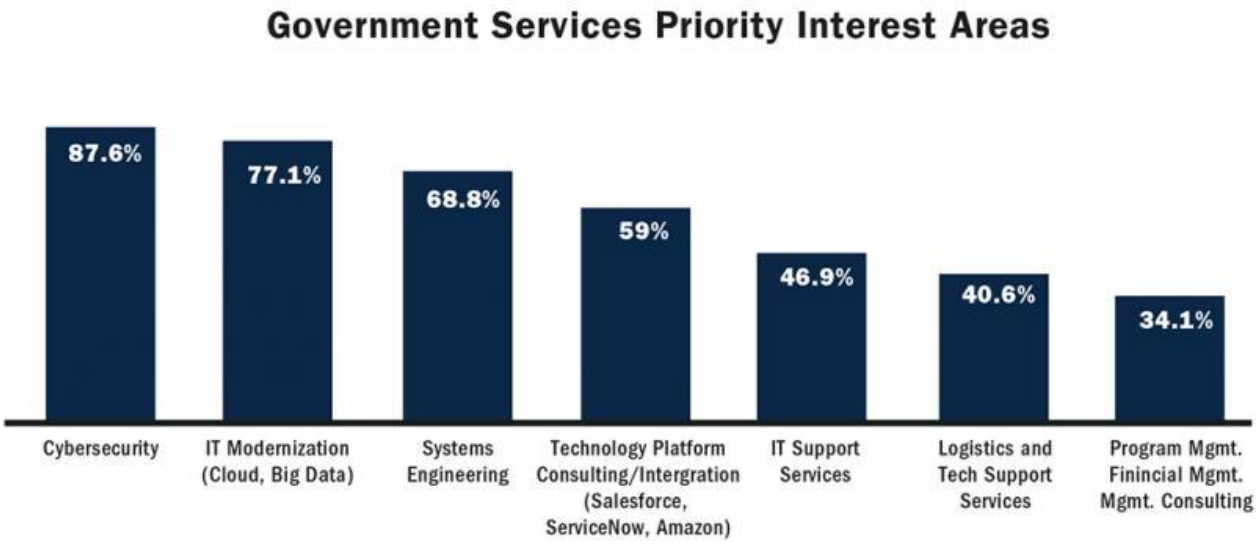



Рис. Р. 2. Пріоритети державних задач

# ДОДАТОК С. ПРОЄКТУВАННЯ ОПИСІВ ФУНКЦІОНАЛЬНИХ ВУЗЛІВ