МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ГОРМАКОВА ІРИНА ВОЛОДИМИРІВНА

УДК 004.315.5

МЕТОДИ СИНТЕЗУ АРИФМЕТИЧНИХ МОДУЛІВ ІЗ ВБУДОВАНОЮ ДІАГНОСТИЧНОЮ ІНФРАСТРУКТУРОЮ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.

Робота виконана на кафедрі автоматики та управління в технічних системах Національного технічного університету «Харківський політехнічний інститут» Міністерства освіти і науки України.

Науковий керівник доктор технічних наук, професор
Дербунович Леонід Вікторович,
Національний технічний університет «Харківський політехнічний інститут»,
професор кафедри автоматики та управління в технічних системах

Офіційні опоненти: доктор технічних наук, професор
Кривуля Геннадій Федорович,
Харківський національний университет радіоелектроніки,
завідувач кафедри автоматизації проектування обчислювальної техніки

кандидат технічних наук, доцент
Кошман Сергій Олександрович,
Харківський національний технічний університет сільського господарства ім. П. Василенка,
доцент кафедри автоматизації та комп'ютерно-інтегрованих технологій

Захист відбудеться "2" липня 2013 р. о 14^{30} годині на засіданні спеціалізованої вченої ради Д 64.050.14 в Національному технічному університеті «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Фрунзе, 21.

З дисертацією можна ознайомитися у бібліотеці Національного технічного університету «Харківський політехнічний інститут» за адресою: 61002, м. Харків, вул. Фрунзе, 21.

Автореферат розісланий "30" травня 2013 року.

Вчений секретар
спеціалізованої вченої ради І.Г. Ліберг

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Стрімкий розвиток інформаційних технологій, широке розповсюдження телекомунікаційних мереж, мереж мобільного зв'язку, а також всесвітньої мережі Internet обумовили необхідність створення комп'ютерних систем (КС) та засобів комунікації, здатних забезпечити швидку та безпечну обробку та передачу інформації. Найкращим рішенням проти несанкціонованого використання інформації є застосування криптографічних систем, що обумовило проведення інтенсивної дослідницької діяльності у галузі вивчення криптографії. Сучасними криптографічними засобами, що гарантують безпеку зв'язку, зберігання та обробки даних в комп'ютерних мережах, є цифровий підпис та аутентифікація користувача на основі пароля.

За останні десятиріччя з'явилося багато робіт, присвячених побудові криптостійких алгоритмів та протоколів, а також програмній та апаратній реалізації різноманітних криптопроцесорів. Дослідження вчених та спеціалістів у галузі синтезу криптосистем доводять, що однією з найбільш трудомістких та часовитратних арифметичних операцій, які складають основу криптоалгоритмів, є операція множення двійкових векторів в скінченних полях. У напрямку аналізу, синтезу та оцінки складності арифметичних алгоритмів в криптосистемах слід відзначити таких вчених: Н. Коблиц, Дж. Дэвенпорт, Венбо Мао, Х.У. Ленстра, А.А. Болотов, А.Г.Ростовцев, А.Н. Черьомушкін, А. А. Белецький, P. Montgomery, H. C. Williams, B. Ansari, M. A. Hasan та інші.

Одним з найбільш розповсюджених засобів «зламу» систем захисту інформації є внесення помилок в процес передавання та обробки даних в криптопроцесорах. Тому використання вбудованих засобів тестового, функціонального діагностування та відновлення працездатності програмно-апаратних засобів криптографічних систем, які включені до засобів діагностичної інфраструктури КС, дозволяє підвищити надійність та достовірність обробки інформації та виключити негативне втручання в процес функціонування криптопроцесорів.

Вагомий внесок у вирішення проблем тестового і функціонального діагностування, генерації тестів і моделювання несправностей, створення вбудованих засобів діагностування зробили вчені П.П. Пархоменко, Е.С. Согомонян, А.П. Горяшко, В.Г. Тоценко, Л.А. Мироновський, Д.В. Сперанський, В.А. Твердохлібов, Г.І. Кривуля, А.М. Романкевич, Л.В. Дербунович, Ю.А. Скобцов, E.J. McCluskey, S.K. Gupta, J.A. Abraham та інші.

В більшості існуючих схем помножувачів у полях $GF(2^p)$ реалізовані алгоритми або прямого помноження елементів поля, або помноження елементів за методом Монтгомері при використанні нормального, поліноміального або подвійного базису представлення елементів скінченного поля. Перспективним є напрямок синтезу гібридних схем помножувачів, що здатні виконувати операцію множення одночасно елементів поля $GF(p)$ та $GF(2^p)$. Проектування універсальних модулів, що об'єднують в собі обчислювальні властивості

помножувачів в скінченних полях при використанні різних алгоритмів множення, дозволяє досягти алгоритмічної гнучкості для цифрових систем захисту інформації та криптопроцесорів.

Таким чином, розробка та удосконалення моделей, методів та процедур синтезу універсальних арифметичних модулів криптографічних систем на сучасній елементній базі із вбудованою діагностичною інфраструктурою, які виконують операцію множення двійкових векторів в полі $GF(2^p)$ та відповідають вимогам мінімальних апаратних витрат та максимальної швидкодії, є актуальною науково-практичною задачею, яка визначила напрямок дисертаційної роботи.

Зв'язок роботи з науковими планами, програмами, темами. Розробка основних положень роботи здійснювалася на кафедрі автоматики та управління в технічних системах НТУ «ХПІ» відповідно до держбюджетної науково-дослідної роботи МОН України «Розробка методів цифрової обробки біомедичних сигналів та зображень» (Д.Р. № 0106U001488) та в рамках госпдоговірної теми «Дослідження та розробка інформаційно-вимірювального стенду для контролю технологічних норм перевірки електричних та часових параметрів спеціалізованих реле» (Українська державна академія залізничного транспорту, м.Харків), де здобувач був виконавцем окремих етапів.

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення рівня контролепридатності та зниження трудомісткості діагностування арифметичних модулів криптографічних систем захисту інформації на основі розробки моделей, методів та процедур синтезу цифрових пристроїв із вбудованими засобами діагностичної інфраструктури сигнатурного моніторингу, які реалізуються на сучасній елементній базі.

Для досягнення сформульованої мети поставлені такі завдання:

– аналіз стану, тенденцій розвитку, методів синтезу та логічного проектування компонентів КС, криптосистем та криптоалгоритмів із вбудованими засобами тестового та функціонального діагностування в світлі сучасних наноелектронних технологій;

– розробка методів та процедур синтезу арифметичних модулів в полях $GF(2^p)$ із блочно-модульною архітектурою на основі використання мереж клітинних автоматів, які виконують операцію послівно-послідовного множення двійкових векторів в полі $GF(2^p)$ та множення елементів поля за методом Монтгомері;

– розробка методів та процедур синтезу універсальних послівно-послідовних модулів множення в полях $GF(2^p)$ із вбудованими засобами тестового діагностування на основі ПЛІС типу FPGA;

– розробка моделей та методів синтезу вбудованих засобів сигнатурного моніторингу на основі гібридних мереж клітинних автоматів;

– застосування розроблених методів синтезу арифметичних модулів в комп’ютерних та інформаційно-керуючих системах.

Об'єкт дослідження – процеси синтезу та логічного проектування компонентів КС із вбудованими засобами сигнатурного моніторингу.

Предмет дослідження – моделі, методи та процедури синтезу арифметичних модулів що легкотестуються із вбудованими засобами генерації перевіряючих тестів і сигнатурного аналізу працездатності.

Методи дослідження. Для вирішення поставлених завдань у роботі використовувалися методи: теорії цифрових автоматів для розробки автоматних моделей і структур арифметичних пристроїв; теорії графів та алгебри регулярних подій для розробки моделей та правил настроювання мережі клітинних автоматів; алгебраїчні методи та процедури сучасної криптографії при розробці структур арифметичних пристроїв, що функціонують в скінченних полях Галуа. Методи технічного діагностування застосовані при розробці засобів тестового діагностування та синтезу генераторів тестових послідовностей, сигнатурних аналізаторів на гібридних мережах клітинних автоматів. Оцінка ефективності розроблених методів та результатів дослідження здійснена на основі комп'ютерних експериментів, отриманих в лабораторних та виробничих умовах при розробці діагностичного програмного комплексу для ПТК СКУ енергоблоку ТЕС.

Наукова новизна отриманих результатів полягає в наступному:

вперше:

- розроблена та обґрунтована автоматна модель клітинного автомата, яка базується на апараті алгебри регулярних подій, що дозволяє спростити обчислювану процедуру аналізу групових властивостей та еволюції мережі, яка складається з гетерогенних ланок із різними правилами налаштування;
- запропоновано та розроблено метод синтезу генераторів детермінованих тестових послідовностей цифрових пристроїв на мережах клітинних автоматів, що дозволяє виключити використання бази тестових даних та спростити апаратну реалізацію генераторів тестів на ПЛІС;
- розроблено та обгрунтовано метод синтезу логічної схеми модуля множення Монтгомері в скінченних полях на основі блочно-модульної структури, що дозволяє модифікувати його схемну реалізацію на ПЛІС типу FPGA при зміні довжини операндів, слова та утворюючого полінома;

отримали подальший розвиток:

- матричні моделі мереж клітинних автоматів, на основі яких визначені необхідні та достатні умови еволюції мережі з властивостями груп, що дозволило генерувати циклічні двійкові послідовності необхідної довжини;
- методи синтезу послівно-послідовних архітектур та алгоритми множення в скінченних полях Галуа, що дозволяє реалізувати схему помножувача з оптимальним співвідношенням показників апаратно-часових витрат;
- методи синтезу універсальних послівно-послідовних помножувачів в полях Галуа із вбудованими генераторами тестових послідовностей та сигнатурних аналізаторів на клітинних автоматах, що забезпечує достовірність обробки даних та спрощує реалізацію помножувачів на ПЛІС.

Практичне значення отриманих результатів в галузі КС та компонентів полягає у вирішенні комплексу завдань, пов'язаних з розробкою і проектуванням універсальних помножувачів в полях Галуа, що реалізуються на

сучасних ПЛІС, відмовостійкість та контролепридатність яких забезпечується вбудованими засобами сигнатурного моніторингу справності складових функціональних модулів помножувача.

Зокрема для систем захисту інформації отримано:

- підвищення достовірності функціонування арифметичних модулів систем захисту інформації, які адаптовані для реалізації на ПЛІС типу FPGA;
- виключення необхідності виконання трудомістких процедур генерації тестів і моделювання несправностей, що знижує витрати на реалізацію системи вбудованого діагностування;
- впровадження методів захисту інформації при розробці діагностичного програмного комплексу для ПТК СКУ енергоблоку ТЕС державним підприємством «Харківський науково-дослідний інститут комплексної автоматизації».

Основні положення дисертаційної роботи використовуються в навчальному процесі на кафедрі автоматики та управління в технічних системах НТУ «ХПІ» при дипломному проектуванні та викладанні дисциплін «Теорія цифрових автоматів», «Експлуатація та забезпечення надійності біомедичних систем».

Особистий внесок здобувача. Основні результати, що виносяться на захист дисертаційної роботи, отримані здобувачем самостійно. Серед них: метод побудови автоматної моделі ланки мережі клітинних автоматів, який базується на апараті алгебри регулярних подій; метод синтезу генераторів детермінованих тестових послідовностей цифрових пристроїв на мережах клітинних автоматів, заснований на виключенні запам’ятовуючих пристроїв із базою тестових даних та спрощені апаратної реалізації генераторів тестів на ПЛІС; декомпозиційний метод та процедура синтезу послівно-послідовних помножувачів Монтгомері у скінченних полях $GF(2^p)$ на основі блочно-модульної архітектури із використанням мереж клітинних автоматів; декомпозиційний метод та процедура синтезу універсальних послівно-послідовних помножувачів у скінченних полях $GF(2^p)$ із вбудованими засобами тестового діагностування; процедури синтезу багатоканальних сигнатурних аналізаторів на основі гібридних мереж клітинних автоматів для використання в діагностичних системах цифрових пристроїв.

Апробація результатів. Основні наукові положення і результати роботи доповідалися й обговорювалися на: XVI, XVII, XVIII, XIX, XX Міжнародних науково-практичних конференціях «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (Харків, 2008, 2009, 2010, 2011, 2012), 22-ій Міжнародній науково-практичній конференції «Перспективные компьютерные, управляющие и телекоммуникационные системы для железнодорожного транспорта Украины» (м. Алушта, Крим, 2009), Другій та Третій Міжнародній науково-практичній конференції «Методи та засоби кодування» (м. Вінниця, 2009, 2011); Міжнародній науково-практичній конференції «Інформаційні технології та комп’ютерна інженерія» (м. Вінниця, 2010), на науково-технічних семінарах кафедри автоматики та управління в технічних системах НТУ «ХПІ».

Публікації. За підсумками наукових досліджень опубліковано 10 наукових праць, в тому числі 7 статей у фахових виданнях України, 3 у матеріалах конференцій.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг роботи становить 216 сторінок. Робота містить: 42 рисунка в тексті та 2 рисунка на 2 окремих сторінках, 27 таблиць в тексті, список використаних джерел із 132 найменувань на 13 сторінках, шість додатків на 36 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обгрунтовано актуальність теми дисертації, сформульовано її мету й задачі, визначено об'єкт, предмет і методи дослідження, наукову новизну і практичну корисність отриманих результатів, стисло характеризується зміст дисертації.

Перший розділ присвячений аналізу стану та тенденцій розвитку методів побудови криптосистем та криптоалгоритмів, що є основою функціонування систем захисту інформації в розподілених комп'ютерних мережах. На сьогодняшній день найбільш вживаними є криптосистеми з відкритим ключем (асиметричні криптосистеми), що функціонують за алгоритмом RSA, або системи на основі еліптичних кривих. Виконання алгоритмів шифрування даних в таких системах здійснюється за допомогою спеціалізованих процесорів, які за своєю сутністю є арифметичними процесорами. Але замість цілочисельної арифметики з плаваючою крапкою криптопроцесор виконує арифметичні операції в скінченних полях. Дослідження показали, що завдяки реалізації криптопроцесорів на високопродуктивних ПЛІС типу FPGA, платформах FPSLIC досягається висока швидкодія при виконанні арифметичних операцій. Наведені переваги криптосистем в еліптичних кривих над полями $GF(2^p)$ порівняно з полями $GF(p)$. Показано, що основою алгоритма обчислення скалярного добутку крапки еліптичної кривої kP є повторення операцій подвоєння та додавання крапки кривої, які в свою чергу базують на операціях множення, додавання та зведення в квадрат в скінченних полях.

Проведений аналіз існуючих архітектур помножувачів на базі ПЛІС типу FPGA (ALTERA, Xilinx) за показниками апаратних та часових витрат показав, що помножувачі з послівно-послідовною архітектурою мають переваги порівняно з паралельною чи побітово-послідовною архітектурою, бо перша архітектура має значні апаратні витрати при виконанні операції множення за один такт, а друга архітектура при досить невеликих апаратних витратах виконує операцію множення за кількість тактів, що дорівнює довжині операнда.

Підвищення надійності та відмовостійкості криптосистем досягається завдяки використанню вбудованих засобів тестового та функціонального діагностування. Сучасна елементна база дозволяє реалізувати вбудовані засоби діагностування відповідно до вимог міжнародного стандарту IEEE P1500. Відмовостійкість та контролепридатність криптосистем забезпечується

використанням для реалізації арифметичних операцій модулів з систолічною структурою без зворотних зв'язків, які легко тестуються, наприклад однорідних структур, зокрема мереж клітинних автоматів.

Внаслідок аналізу структурної організації, методів синтезу криптосистем і проектування їх компонентів із вбудованими засобами діагностики обгрунтовані і сформульовані мета і завдання дисертаційної роботи.

Другий розділ присвячений розробці методів та процедур побудови регулярної граматики по кінцево-автоматній моделі ланки мережі клітинних автоматів з метою знаходження множини регулярних виразів, які відповідають різним правилам налаштування ланки мережі.

Одновимірна мережа клітинних автоматів (МКА) являє собою упорядкований масив однорідних ланок, кожна *i*-та ланка в момент часу *t* може приймате одне з допустимих значень із алфавіту $S=\{0, 1, \ldots, k\text{-}1\}$, де k – кількість допустимих станів ланки. На кожному такті функціонування МКА обчислює новий стан кожної ланки в залежності від станів $(2r+1)$ сусідніх ланок у відповідності до визначеного правила $f{:}S^{2r+1}\rightarrow S$, де r – кількість вимірів мережі.

Визначення 1. Множина станів усіх ланок мережі в момент часу *t* визначає стан всієї МКА в момент часу *t* та позначається як $A^{(t)}$.

Показано, що функціонування МКА визначається відображенням $f{:}A^{(t)}\rightarrow A^{(t+1)}$ поточного стану $A^{(t)}$ в наступний стан $A^{(t+1)}$. Множина станів МКА після *t* тактів функціонування $\Omega^{(t)}=\{A^{(0)}, A^{(1)}, \ldots, A^{(t)}\}$ є формальною мовою, в якій кожне допустиме слово представлене станом МКА $A^{(i)}$. Обгрунтовано, що безкінечну множину двійкових векторів, що генеруються МКА, можливо описати за допомогою визначеного набору граматичних правил.

Розроблена кінцево-автоматна модель ланки МКА, яка є автоматом Мура. Вхідним алфавітом автомата $X=\{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$ є множина можливих поєднань станів самої клітини та її найближчих сусідів зправа та зліва, де x_0=000, x_1=001, x_2=010, x_3=011, x_4=100, x_5=101, x_6=110, x_7=111. Множина станів автомата визначається як $Z=\{z_0, z_1\}$, де z_0=0, z_1=1. Вихідний алфавіт кінцевого автомата *Y* складається з множини символів {0; 1}. Функції переходів кінцевого автомату визначаються правилом налаштування ланки МКА: $\delta(z_i, x)=\{z_j: z_i\rightarrow_x z_j\}$. Функції переходів на впорядкованій парі (стан ланки z^0_t, стан сусіда зліва z^1_t та сусіда зправа z^{-1}_t) відповідає стану ланки z^0_{t+1}.

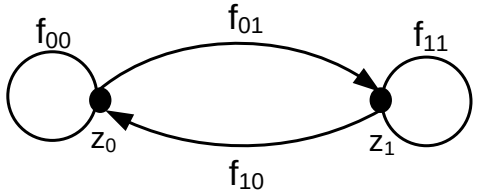


Рис.1. Граф переходів абстрактного кінцевого автомата

Використання алгебри регулярних подій дозволило розробити процедуру знаходження системи алгебраїчних рівнянь (1), яка повністю описує поведінку клітинного автомата, автоматна модель якого задана графом переходів рис. 1. Для спрощення позначень диз'юнкція вхідних слів, які переводять автомат зі стану z_0 в стан z_0, позначається як функція f_{00}, відповідно зі

стану z_0 в стан z_1 – як функція f_{01}, за стану z_1 в стан z_1 – як функція f_{11} та зі стану z_1 в стан z_0 – як функція f_{10}.

$$\begin{cases} R_{00} = \left[f_{00} + f_{01}\{f_{11}\}^* f_{10} \right]^*, \\ R_{01} = \left[f_{00} + f_{01}\{f_{11}\}^* f_{10} \right]^* \cdot f_{01} \cdot \{f_{11}\}^*, \\ R_{10} = \left[f_{11} + f_{10}\{f_{00}\}^* f_{01} \right]^* \cdot f_{10} \cdot \{f_{00}\}^*, \\ R_{11} = \left[f_{11} + f_{10}\{f_{00}\}^* f_{01} \right]^*. \end{cases} \quad (1)$$

Отримана система рівнянь є системою регулярних виразів, що визначають множину слів, які допускаються кінцевим автоматом та переводять автомат зі стану z_i в z_j. Тобто система рівнянь (1) визначає регулярну мову кінцево-автоматної моделі ланки МКА. Отримана кінцево-автоматна модель ланки МКА не залежить від правила функціонування ланки (лінійне чи нелінійне) та дозволяє вирішити задачу аналізу поведінки ланки МКА.

МКА, яка складається з n ланок, має кінцеву кількість можливих станів 2^n. Показано, що роботу такої МКА можливо представити або у вигляді графа переходів станів, або матрицею переходів. Визначено операцію МКА як перехід МКА зі стану $A^{(t)}$ в стан $A^{(t+1)}$.

Визначення 2. МКА, яка складається з n ланок, є такою алгебраїчною системою, носієм якої є множина всіх можливих станів МКА $G=\{g_0\, g_1 \ldots g_{2^n-1}\}$, а сигнатурою є операція МКА (*), що визначається відображенням f: $G \to G$ множини переходів поточних станів МКА в наступні стани на кожному такті роботи.

Сформульоване та доведене наступне твердження.

Твердження 1. Нехай задана МКА, граф переходів якої містить множину циклів. Тоді будь-яка подстановка Q вида $Q=(\alpha_0\ \alpha_1 \ldots \alpha_k)$, де $\{\alpha_0\ \alpha_1 \ldots \alpha_k\}$ – множина станів, які належать до одного циклу графа переходів МКА, формує групу $G'=(G, \Omega, \Pi)$, носієм якої є множина $G=\{\alpha_0\ \alpha_1 \ldots \alpha_k\}$ та множина операцій Ω складається з операції МКА (*).

Визначені необхідні та достатні умови еволюції МКА із властивостями груп та формування циклічних двійкових послідовностей необхідної довжини. Всі лінійні правила налаштування МКА в залежності від початкового стану ланок та граничних умов дозволяють генерувати циклічні послідовності різної довжини, які формують групи за операцією МКА (*).

Розроблено метод та процедуру синтезу генераторів детермінованих послідовностей на основі МКА, що базується на принципі зміни функціонального налаштування ланки МКА у відповідності до набору перевіряючи послідовностей.

Третій розділ присвячений розробці методів та процедур синтезу помножувачів в скінченних полях Галуа $GF(2^p)$. Обгрунтовано вибір послівно-послідовної архітектури для реалізації помножувачів елементів скінченного поля на основі критерію мінімальних апаратних витрат та максимальної швидкодії. При такій архітектурі один з операндів подається на схему

помножувача повністю, а інший розбивається на $\lceil p/\omega \rceil = k$ слів довжиною ω біт та подаєть на схему множення послівно.

Нехай у скінченному полі $GF(2^p)$ існує елемент α, що утворює всі ненульові елементі поля $\{\alpha, \alpha^2, \ldots, \alpha^{2^p-1}\}$ та поліном $F(x)=x^p+f_{p-1}x^{p-1}+ +f_{p-2}x^{p-2}+\ldots+f_1x+1$, $f_i \in GF(2)$, є утворюючим поліномом поля.

Визначення 3. Помножувачем першого роду називається помножувач, який обчислює добуток двох елементів скінченного поля $A, B \in GF(2^p)$ згідно виразу

$$C_1 = A \times B \bmod F(\alpha), \tag{2}$$

де $F(\alpha)$ – поліном, який утворює поле $GF(2^p)$, що не приводиться.

Визначення 4. Помножувачем другого роду (Монтгомері) називається помножувач, який обчислює добуток двох $F(\alpha)$-лишкі $A, B \in GF(2^p)$ елементів скінченного поля $A', B' \in GF(2^p)$ згідно виразу

$$C_2 = AB\, R^{-1} \bmod F(\alpha), \tag{3}$$

де R – поліном, який відповідає умові НСД(R, $F(\alpha)$)=1.

$F(\alpha)$-лишки елементів скінченного поля $A', B' \in GF(2^p)$ обчислюються згідно виразів:

$$A = A' \cdot R \bmod F(\alpha) = \sum_{i=0}^{p-1} a_i \alpha^i, \tag{4}$$

$$B = B' \cdot R \bmod F(\alpha) = \sum_{i=0}^{p-1} b_i \alpha^i. \tag{5}$$

Розглянуті та наведені основні алгоритми множення в скінченних полях та відповідні їм структурні схеми помножувачів першого роду при апаратній реалізації. Проведено оцінку апаратних та часових витрат для різних видів архітектур помножувачів (табл. 1).

Таблиця 1

Порівняння архітектур помножувачів в скінченних полях

Архітектура	Час виконання	Апаратні витрати ($F(x)=x^p+x^d+1$)	
Побітово-послідовне множення	p	AND: p	XOR: $p+1$
Блочно-послідовне множення	$\lceil p/\omega_1 \rceil + \lceil p/\omega_2 \rceil$	AND: $2\omega_1\omega_2$	XOR: $2\omega_1\omega_2$
Послівно-послідовне множення	$\lceil p/\omega_1 \rceil$	AND: $\omega_1 p$	XOR: $\omega_1(p+1)$
Паралельне множення	1	AND: p^2	XOR: $(p-1)(p+1)$
ω_1 – довжина слова в бітах; ω_2 – довжина блока в бітах.			

Розроблено процедуру синтезу послівно-послідовного помножувача першого роду із блочно-модульною архітектурою, який обчислює добуток елементів поля $A, B \in GF(2^p)$ згідно виразу

$$\begin{aligned} C_1 = AB \bmod F(\alpha) &= [(\ldots(A_{k-1}\alpha^\omega + A_{k-2})\alpha^\omega + \ldots + A_1)\alpha^\omega + A_0]B \bmod F(\alpha) = \\ &= [(\ldots(A_{k-1}B\alpha^\omega + A_{k-2}B)\alpha^\omega + \ldots + A_1B)\alpha^\omega + A_0B] \bmod F(\alpha), \end{aligned} \tag{6}$$

де ω – довжина слова в бітах; A_j – поліном ступеня $\le(\omega-1)$, $j=0,\ldots,(k-1)$.

Запропоновано та обгрунтовано використання мереж клітинних автоматів для реалізації модуля, що обчислює частковий добуток згідно виразу

$$D_i=A_jB=a_0B+a_1B\alpha+a_2B\alpha^2+\ldots+a_{\omega-1}B\alpha^{\omega-1}, \quad (7)$$

де A_j – чергове слово першого операнда.

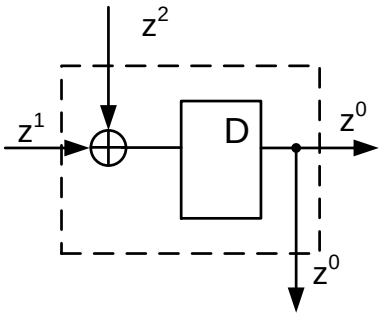


Рис. 2. Ланка МКА

Кожна МКА є однорідною мережею, яка складається з p ланок $[z_0, z_1, \ldots, z_{p-1}]$. Вихід ланки z_{p-1} заводиться на вхід нульової ланки. Відповідно, правило функціонування для ланки z_0 має вигляд: $z_0(t+1)=z_{p-1}(t)$. Решта ланок $z_1,\ldots, z_{p-1}$ мають однакову структуру (рис. 2). Кожна ланка пов'язана з сусідом зліва z^1, окрім цього, в кожну ланку додано верхній вхід z^2. На верхній вхід z^2 i-ої ланки подається вихідний сигнал $(p-1)$-ої ланки тільки в тому разі, коли коефіцієнт f_i утворюючого полінома $F(\alpha)$ дорівнює 1. Правило функціонування ланки в такому разі має вигляд $z^0{}_{(t+1)}=z^1{}_t\oplus z^2{}_t$. При $f_i=0$ правило функціонування ланки дорівнює $z^0{}_{(t+1)}=z^1{}_t$.

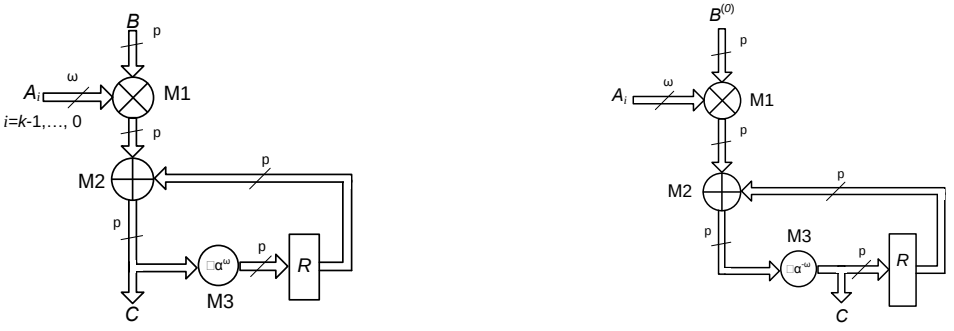
Для помножувачів другого роду запропоновано визначати добуток елементів поля згідно виразу

$$C_2=[(\ldots(A_0B^{(0)}\alpha^{-\omega}+A_1B^{(0)})\alpha^{-\omega}+\ldots+A_{k-1}B^{(0)})\alpha^{-\omega}]\bmod F(\alpha), \quad (8)$$

де $B^{(0)}=B\cdot\alpha^{(k\omega-u)}$.

Розроблено процедуру синтезу послівно-послідовного помножувача другого роду, що має блочно-модульну архітектуру, із використанням уніфікованих блоків, використаних в помножувачі першого роду.

Аналіз запропонованих процедур синтезу помножувачів першого та другого роду показав, що алгоритми визначення добутку для обох типів помножувачів мають спільні операції та можуть бути реалізовані за допомогою однакових уніфікованих модулів (рис. 3).



а) б)

Рис. 3. Структурні схеми послівно-послідовних помножувачів першого (а) та другого роду (б)

Блок М1 на рис. 3 призначений для обчислення часткового добутку (5) та реалізован за допомогою МКА, мереж з p AND вентилів та мережі з p XOR вентилів. Блок М2 реалізован за допомогою p двовхідних XOR вентилів. Блок М3 призначений для обчислення добутку $Y=L\cdot\alpha^{\omega}\bmod F(\alpha)$ (рис. 3 а) або $Y=L\cdot\alpha^{\omega}\bmod F(\alpha)$ (рис. 3 б) та представляє собою спеціальним чином побудовану мережу з XOR вентилів.

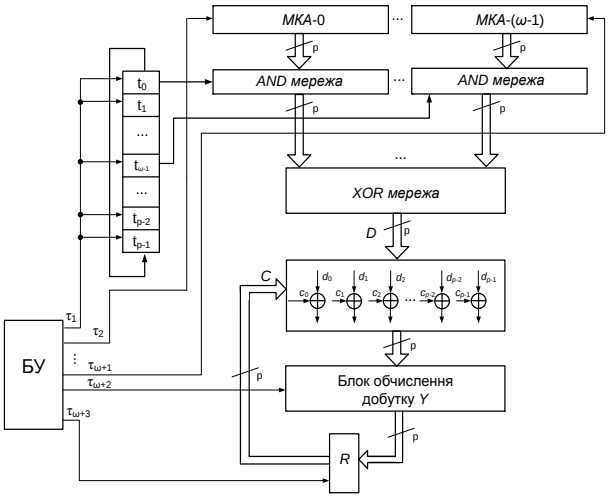


Рис.4. Архітектура універсального помножувача в скінченних полях $GF(2^p)$

Запропоновано та обґрунтовано декомпозиційний метод синтезу універсального помножувача в скінченних полях, який дозволяє отримати структуру, що об'єднує в собі обчислювальні властивості помножувачів обох типів (рис. 4). Блок обчислення добутку Y в запропонованій архітектурі має структуру, що легко реконфігурується та дозволяє в залежності від управляючого сигналу $\tau_{\omega+2}$ обчислювати або добуток $Y=L\cdot\alpha^{-\omega}\bmod F(\alpha)$, або $Y=L\cdot\alpha^{\omega}\bmod F(\alpha)$ (рис. 5).

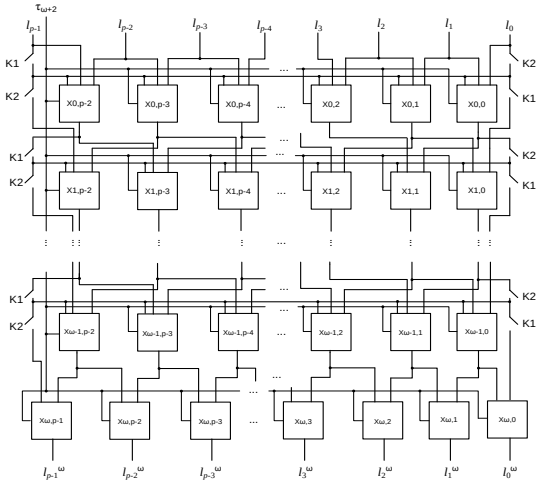


Рис. 5. Структура блока обчислення добутку Y

Визначено час виконання однієї операції множення, який складає $(\lceil p/\omega\rceil+\omega)$ тактів.

Використання уніфікованих блоків позволяє легко реалізувати отриману архітектуру універсального помножувача на ПЛІС типу FPGA та без додаткових обчислень модифікувати структуру помножувача при зміні довжини операндів, довжини слова чи полінома, що утворює поле. Зміна утворюючого полінома при збереженні ступеня полінома p потребує зміни правил настроювання мереж клітинних автоматів при повному збереженні загальної структури.

Для комп'ютерного дослідження та порівняння характеристик отриманої апаратної реалізації помножувача з існуючими результатами розроблено схемну реалізацію універсального помножувача на ПЛІС типу FPGA XC5VLX330-2FF1760 фірми Xilinx із використанням засобів середовища розробки ISE Design Suit 14.3.

Для синтезу помножувача в полі $GF(2^{163})$ обран утворюючий поліном $F(x)=x^{163}+x^7+x^6+x^3+1$, довжина слова склала $\omega=8$ біт та кількість слів для $p=163$ визначається як $k=\lceil p/\omega\rceil=\lceil 163/8\rceil=21$. Отримані наступні результати синтезу за апаратними витратами (табл. 2).

Таблиця 2

Апаратні витрати

Найменування	Використано	Доступно	У % відносно загальної кількості
регістри	1474	408000	0
КЛБ	1971	204000	0
пара КЛБ-тригер	1470	1975	74
входи/виходи	346	600	57

Отримані результати порівнювалися із запропонованою Б. Ансарі архітектурою, яка була реалізована на FPGA фірмы Xilinx Virtex 4 XC4VLX200. В архітектурі Б. Ансари всі поточні операції виконувалися без приведення за модулем та обчислення остаточного результата множення виконувалося за допомогою додаткового модуля при наступних апаратних витратах:

- кількість використаних регістрів – 4080;
- кількість використаних тригерів – 1502;
- КЛБ – 7719.

Також розроблена архітектура помножувача дозволяє раціонально використовувати апаратні можливості обраної FPGA – повністю використані пари КЛБ-тригер склали 74 %.

Четвертий розділ присвячений синтезу архітектури універсального помножувача в скінченних полях $GF(2^p)$ із вбудованими засобами тестового діагностування, які забезпечують перевірку справності схеми в режимах мікродіагностики – в проміжках між періодами функціонування схеми (рис. 6).

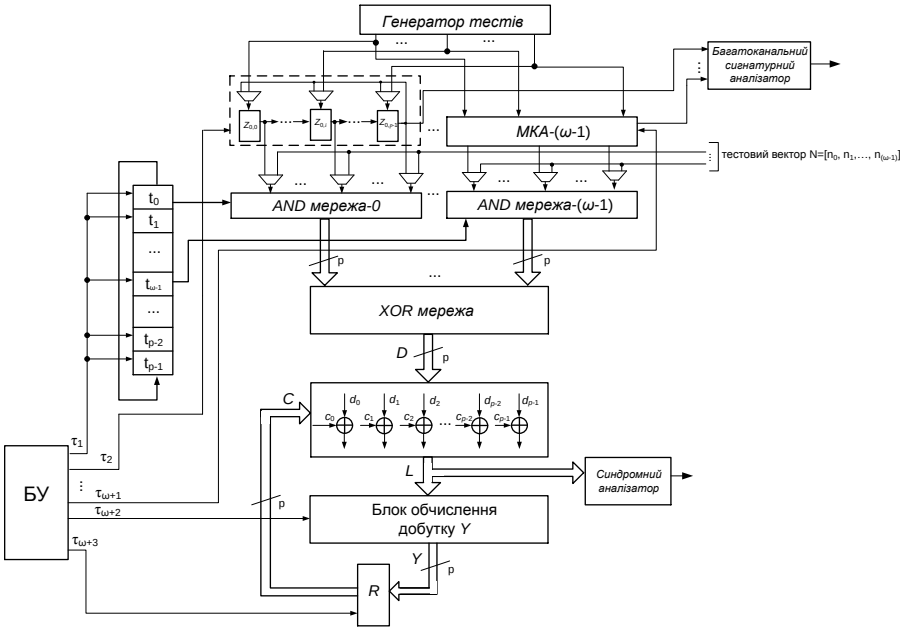


Рис. 6. Архітектура універсального помножувача з вбудованими засобами тестового діагностування

Для вирішення задачі тестового діагностування запропоновані методи синтезу генераторів тестових послідовностей для кожного складового модуля помножувача, що виявляють клас константних несправностей. Процес

тестування схеми розділено на два паралельних потока: 1) тестування комбінаційної частини схеми (XOR мережа, модуль обчислення суми проміжного результата, AND мережі, модуль обчислення добутку *Y*); 2) тестування елементів з пам'ятю (МКА, зсувний регістр, регістр *R*).

Визначені та обґрунтовані тестові послідовності, необхідні для прийняття рішення про справність комбінаційної частини схеми помножувача, які подаються на входи AND мереж (рис. 6). Біти вектора *N* на першому, другому та третьому такті тестового діагностування відповідно дорівнюють: 1) n_0=0, n_i=1 для i=1…(ω-1); 2) n_0=1, n_i=0 для i=1…(ω-1); 3) n_i=1 для i=0…(ω-1). Синдром двійкової послідовності, що знімається з модуля обчислення проміжних результатів, порівнюється з еталонним синдромом.

Для побудови діагностичного експерименту для МКА, яка розглядається як однорідна одномірна мережа без спостережуваних виходів, її ланка представляється таблицею істинності автомата Мура (табл. 3).

Обгрунтовано та доведено теореми, які визначають необхідні та достатні умови існування перевіряючи тестових наборів x_T для однорідної мережі.

Теорема 1. Нехай правий вихід ланки C_k одномірної однорідної мережі знаходиться у стані z_j та до верхніх входів ланок C_{k+1}, C_{k+2}, …, C_{p-1} прикладений вхідний набір $X_k = (x_{k+1}, x_{k+2}, ..., x_{p-1})$, який викликає послідовність переходів станів ланок мережі у вигляді $z_j \xrightarrow{x_{\kappa+1}} z_{\kappa+1} \xrightarrow{x_{\kappa+2}} z_{\kappa+2} \xrightarrow{x_{\kappa+3}} ... z_{p-1} \xrightarrow{x_{p-1}} z_{p-1}$, де стан стан зліва від вхідного символу $x_j \in x_\alpha$, $\alpha = (k+1)(k+2)...$, що є попереднім, а стан зправа від x_α – наступним. Якщо існує послідовність станів ланок состояний ячеек C_{k+1}, C_{k+2}, …, C_{p-1}, породжувана прикладанням вхідного набору X_k, в якій кожен символ $x_\alpha \in X_k$ є відмітним символом попереднього стану, то послідовність цих символів утворює перевіряючий тестовий набір станів z_j ланки C_k мережі.

Теорема 2. Якщо у ланці однорідної мережі з *n* станами кожен стан має принаймні один відмітний символ, то для такої мережі існує щонайменше одна циклічна відмітна послідовність.

Якщо ланки мережі відповідають вимогам теорем 1 та 2, то така мережа є такою, що легко тестується, та для неї спрощується процедура побудови діагностичного експерименту. Розроблено процедуру знаходження тестових послідовностей, що виявляють несправності класу F_1, для МКА на основі побудови характеристичного і синхронізуючого дерев-наступників для автоматної моделі ланки мережі (рис. 7), визначення з синхронізуючого дерева множини характеристичних шляхів, які починаються з кожного характеристичного символу.

Показано, що для поліпшення показників спостереження та управління в процесі діагностичного експерименту одномірної однорідної мережі без спостережуваних виходів ланка мережі повинна мати управляючий верхній вхід. Окрім цього, діагностичний експеримент для однорідної мережі, що

перевіряється, виконується в два етапи відповідно з двома напрямками розповсюдження сигналів. Для генерації тестових послідовностей до схеми помножувача включений спеціальний генератор, а для аналізу вихідних сигналів, які знімаються з (p-1)-ої ланки МКА запропоновано використання багатоканального сигнатурного аналізатора.

Таблиця 3

Таблиця переходів ланки

z(t)	z(t+1)	
	x=0	x=1
z_0	z_0	z_1
z_1	z_1	z_0

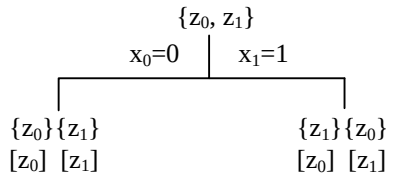
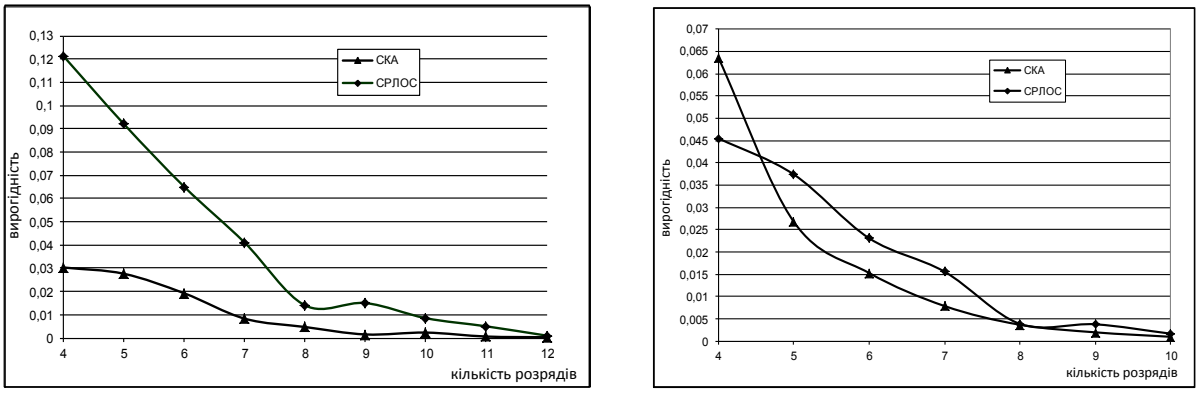


Рис. 7. Характеристичне дерево ланки мережі

Розроблені методи та процедури синтезу одноканальних та багатоканальних сигнатурних аналізаторів на МКА, що базуються на еквівалентності характеристичних матриць МКА та зсувних регістрів з лінійним зворотнім зв'язком (ЗРЛЗЗ). Визначено та обґрунтовано, що всі властивості ЗРЛЗЗ як генератора послідовностей максимальної довжини ізоморфні адитивним МКА, ЗРЛЗЗ є одним з варіантів налаштування адитивної МКА з нульовими граничними умовами.

Розроблено та проведено комп'ютерне дослідження достовірності синтезованих структур одноканальних та багатоканальних сигнатурних аналізаторів на МКА. Визначено, що одноканальні сигнатурні аналізатори на мережах клітинних автоматів мають однакову достовірність знаходження несправностей класу F_1, F_2, F_3 з сигнатурними аналізаторами на ЗРЛЗЗ. Показано, що вирогідність невиявлення помилок в послідовностях, що аналізуються, за допомогою багатоканального сигнатурного аналізатора на МКА значно нижча, ніж за допомогою сигнатурного аналізатора на ЗРЛЗЗ для класу несправностей F_2 (рис. 8а) та F_3 (рис. 8б).



а) б)

Рис. 8. Вирогідність невиявлення двократної (а) та трикратної (б) несправності

Для проведення порівнювального аналізу отриманих архітектур універсального помножувача розроблено схемну реалізацію універсального помножувача із вбудованою діагностичної інфраструктурою на ПЛІС типу FPGA XC5VLX330-2FF1760 фірми Xilinx з використанням засобів середовища розробки ISE Design Suit 14.3. Отримані наступні результати синтезу за апаратними витратами (табл. 4).

Таблиця 4

Апаратні витрати

Найменування	Використано	Доступно	У % відносно загальної кількості
регістри	1809	408000	0
КЛБ	2794	204000	1
пара КЛБ-тригер	1805	2798	64
входи/виходи	359	600	59

Дані таблиць 2 та 4 свідчать, що додаткові апаратні витрати на діагностичну інфраструктуру склали 20% для пар КЛБ-тригер та 40% для КЛБ. Використання алгоритмів оптимізації при трасуванні схеми в FPGA дозволяють скоротити наведені показники.

Експериментальні дослідження підтвердили високу ефективність реалізації запропонованої архітектури універсального помножувача в скінченних полях на ПЛІС типу FPGA завдяки використанню уніфікованих блоків.

У **додатках** наведено докази теорем, текст комп'ютерної програми на мові С++, що реалізує обчислення достовірності одноканальних та багатоканальних сигнатурних аналізаторів на МКА, та тексти вихідних файлів проектів у середовищі Active-HDL 8.2 запропонованих схем помножувачів. Також наведені акти впровадження в ДП «Харківський науково-дослідний інститут комплексної автоматизації» та в навчальний процес кафедри автоматики та управління в технічних системах НТУ «ХПІ».

ВИСНОВКИ

Підсумком дисертаційної роботи стало вирішення науково-практичної задачі підвищення рівня контролепридатності та зниження трудомісткості діагностування арифметичних модулів криптографічних систем захисту інформації на основі розробки моделей, методів та процедур синтезу цифрових пристроїв із вбудованими засобами діагностичної інфраструктури сигнатурного моніторингу, які реалізуються на сучасній елементній базі.

Основні наукові та практичні результати полягають у наступному:

1. На основі аналізу науково-технічних джерел, стану та тенденцій розвитку програмно-апаратних засобів криптографічних систем захисту інформації в розподілених комп'ютерних мережах у світлі сучасних наноелектронних технологій обґрунтована актуальність проектування компонентів КС – арифметичних модулів, які реалізуються на високопродуктивних ПЛІС типу FPGA та легко тестуються.

2. Разроблено метод аналізу стану та налаштування клітинного автомату на основі використання теорії графів та апарату алгебри регулярних подій. Запропоновано та обгрунтовано перспективний метод побудови автоматної моделі ланки МКА, який дозволяє спростити обчислювальну процедуру аналізу еволюції гібридної мережі.

3. Розроблено метод синтезу генераторів детермінованих послідовностей на МКА, який базується на принципі зміни функціональних налаштувань ланок мережі у відповідності до набору перевіряючи послідовностей. Показано, що запропонований метод генерації тестів дозволяє скоротити апаратні витрати за рахунок виключення зі схеми генератора запам'ятовуючих пристроїв, які призначені для зберігання бази тестових даних.

4. Запропоновано та розроблено процедуру синтезу логічної схеми помножувача Монтгомері в скінченних полях $GF(2^p)$. Отримана блочно-модульна архітектура дозволяє модифікувати схемну реалізацію помножувача на ПЛІС типу FPGA при зміні довжини операндів, слова та утворюючого полінома.

5. Запропоновано та розроблено процедуру синтезу універсальних послівно-послідовних помножувачів у скінченних полях $GF(2^p)$ із вбудованими засобами тестового діагностування. Отримана блочно-модульна архітектура поєднує в собі обчислювальні властивості помножувачів Монтгомері та помножувачів, які виконують операцію прямого множення двійкових векторів в скінченному полі. Проведена оцінка апаратних витрат на реалізацію розробленої схеми, що підтверджує ефективність синтезу універсального послівно-послідовного помножувача із вбудованою діагностичною інфраструктурою на ПЛІС типу FPGA.

6. Розроблено метод знаходження тестових наборів для всіх складових блоків універсального послівно-послідовного помножувача. Запропоновано метод синтезу генератора тестових послідовностей для МКА на основі використання відмітних та характеристичних символів автоматної моделі ланки мережі.

7. Розроблені методи та процедури синтезу одноканальних та багатоканальних сигнатурних аналізаторів на МКА, що базуються на еквівалентності характеристичних матриць мережі та ЗРЛЗЗ. Отримана оцінка достовірності знаходження несправностей класу F_1, F_2, F_3 синтезованими структурами одноканальних та багатоканальних сигнатурних аналізаторів на МКА. Показано, що достовірність знаходження несправностей класу F_2, F_3 вище на 2÷4 % у сигнатурних аналізаторів на МКА у порівнянні з аналізаторами на зсувних регістрах.

8. Результати дисертаційної роботи впроваджені в навчальний процес кафедри автоматики та управління в технічних системах НТУ «ХПІ»; при розробці діагностичного програмного комплексу для ПТК СКУ енергоблоку ТЕС державним підприємством «Харківський науково-дослідний інститут комплексної автоматизації».

СПИСОК ОПУБЛІКОВАНИХ РОБІТ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Гормакова И.В. Генераторы детерминированных тестов на клеточных автоматах / И.В Гормакова, Л.В. Дербунович // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2006. – № 31 – С.38-41.

Здобувачем запропоновано метод синтезу генераторів тестів на мережах клітинних автоматів, які реалізують встановлену множину детермінованих тестів при мінімальних апаратних та часових витратах.

2. Гормакова И.В. Алгебраические свойства одномерных сетей клеточных автоматов / И.В Гормакова, Л.В. Дербунович, И.Г. Либерг // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2007. – № 10 – С.71-75.

Здобувачем обґрунтовані необхідні та достатні умови побудови арифметичних модулів на мережах клітинних автоматів, засновані на використанні групових властивостей клітинних автоматів.

3. Гормакова И.В. Вычислительные свойства сетей клеточных автоматов / И.В Гормакова // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2008. – № 56 – С.53-56.

Здобувачем розроблено модель детермінованого кінцевого автомата для ланки мережі клітинних автоматів.

4. Гормакова И.В. Методы анализа поведения сетей клеточных автоматов / И.В Гормакова, А.С. Швецова // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2009. – № 23 – С.50-55.

Здобувачем запропоновано метод та алгоритм аналізу поведінки мережі клітинних автоматів із заданими правилами налаштування ланки мережі, а також алгоритм виділення мереж клітинних автоматів з певними властивостями.

5. Гормакова И.В. Диагностические эксперименты в системах защиты информации на сетях клеточных автоматов / И.В. Гормакова, М.А. Бережная, Я.Ю. Королева // Інформаційно-керуючі системи на залізничному транспорті. – Харків: УкрДАЗТ, 2009. – №4. – С. 142-145.

Здобувачем запропоновано процедуру знаходження тестових послідовностей для модифікованої ланки мережі клітинних автоматів, що базується на використанні циклічних відмінних та характеристичних символів.

6. Гормакова И.В. Методы построения арифметических модулей, оперирующих в полях Галуа / И.В Гормакова, Л.В. Дербунович // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2010. – №23 – С.34-49.

Здобувачем запропоновано процедуру синтезу послівно-послідовного помножувача в полях Галуа $GF(2^p)$, що дозволяє синтезувати архітектуру помножувача, яка відповідає вимогам швидкодії, тестопридатності та гнучкості.

7. Гормакова И.В. Методы синтеза умножителей Монтгомери в полях Галуа с блочно-модульной архитектурой / И.В Гормакова, Р.М. Алиев // Вісник Національного технічного університету «Харківський політехнічний інститут». – Харків: НТУ «ХПІ», 2012. – №37 – С.16-23.

Здобувачем запропоновано процедуру синтезу помножувача Монтгомері в полі Галуа GF(2^p) з блоково-модульною архітектурою, що виконує операцію послівно-послідовного множення елементів поля.

8. Гормакова И.В. Применение сетей клеточных автоматов в криптографических системах / И.В. Гормакова, М.А. Бережная, Я.Ю. Королева // Тези доповідей другої міжнародної науково-практичної конференції «Методи та засоби кодування, захисту та ущільнення інформації», (Вінниця, 22-24 квітня 2009 р.). – Вінниця: ВНТУ, 2009. – С. 94-95.

Здобувачем запропоновано алгоритм синтезу перевіряючих тестів для гібридних мереж клітинних автоматів, які мають групові властивості.

9. Гормакова И.В. Методы синтеза пословно-последовательных умножителей, оперирующих в полях Галуа / И.В. Гормакова // Тези доповідей Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія», (Вінниця, 19-21 травня 2010 р.). – Вінниця: ВНТУ, 2010. – С. 297-298.

Здобувачем сформульовані вимоги до тестопридатності помножувачів в полях Галуа та розроблено алгоритм синтезу перевіряючи тестів для складових блоків послівно-послідовного помножувача в полі GF(2^p).

10. Гормакова И.В. Синтез умножителей в конечных полях с встроенными средствами сигнатурного мониторинга / И.В. Гормакова, Л.В. Дербунович // Тези доповідей третьої міжнародної науково-практичної конференції «Методи та засоби кодування, захисту та ущільнення інформації», (Вінниця, 20-22 квітня 2011 р.). – Вінниця: ВНТУ, 2011. – С. 20-21.

Здобувачем запропоновано метод синтезу багатоканального сигнатурного аналізатора на основі мереж клітинних автоматів, заснований на ізоморфізмі зсувних регістрів з лінійним зворотнім зв'язком та адитивних гібридних мереж клітинних автоматів.

АНОТАЦІЇ

Гормакова І.В. Методи синтезу арифметичних модулів із вбудованою діагностичною інфраструктурою для систем захисту інформації. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний технічний університет «Харківський політехнічний інститут», Харків 2013.

Дисертація присвячена розробці методів та процедур синтезу універсальних помножувачів на ПЛІС типу FPGA із вбудованою діагностичною інфраструктурою, які виконують операцію множення елементів поля *GF*(2^p).

Розглянуті алгоритми та методи реалізації операції множення в скінченних полях $GF(2^p)$. Досліджені обчислювані властивості мереж клітинних автоматів та обґрунтована можливість їх використання при побудові базових арифметичних модулів для криптосистем.

Отримали подальший розвиток методи синтезу послівно-послідовних помножувачів елементів скінченних полів $GF(2^p)$ на основі блочно-модульної архітектури із використанням мереж клітинних автоматів. Обгрунтовано, що послівно-послідовна архітектура найкращим чином відповідає співвідношенню апаратних та часових витрат.

Запропоновано новий метод синтезу логічної схеми послівно-послідовного помножувача Монтгомері в скінченних полях на основі блочно-модульної архітектури з урахуванням реалізації синтезованої схеми на ПЛІС типу FPGA.

Вперше запропоновано декомпозиційний метод та процедуру синтезу універсального послівно-послідовного помножувача в полях Галуа $GF(2^p)$ із вбудованими засобами тестового діагностування. Отримана архітектура поєднує обчислювальні властивості помножувачів Монтгомері та помножувачів, які виконують пряме множення елементів скінченного поля.

Наведені результати експериментальних досліджень синтезованих архітектур помножувачів за апаратними витратами.

Розроблені методи та процедури синтезу одноканальних та багатоканальних сигнатурних аналізаторів на мережах клітинних автоматів, які основані на еквівалентності характеристичних матриць мереж клітинних автоматів та зсувних регістрів з лінійними зворотніми зв’язками. Вперше запропоновано метод синтезу генераторів тестових послідовностей на мережах клітинних автоматів, який дозволяє виключити використання бази тестових даних на запам’ятовуючих пристроях та спростити апаратну реалізацію генераторів тестів на ПЛІС.

Ключові слова: комп’ютерні системи і мережі, мережі клітинних автоматів, система захисту інформації, множення в скінченних полях, послівно-послідовна архітектура, тестове діагностування, сигнатурний аналізатор.

Гормакова И.В. Методы синтеза арифметических модулей с встроенной диагностической инфраструктурой для систем защиты информации. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Национальный технический университет «Харьковский политехнический институт», Харьков 2013 г.

Диссертация посвящена разработке методов и процедур синтеза универсальных умножителей на ПЛИС типа FPGA со встроенной диагностической инфраструктурой, выполняющих операцию умноження элементов поля $GF(2^p)$.

В диссертации обоснована цель, актуальность направления исследования, проведен обзор криптоалгоритмов, на сегодняшний день применяемых

наиболее часто в системах защиты информации, а также известных методов и технологий реализации арифметических модулей в криптографических системах. Рассмотрены алгоритмы и методы реализации операции умножения в конечных полях $GF(2^p)$ – наиболее трудоемкой и аппаратно затратной арифметической операции при выполнении криптоалгоритмов в эллиптических кривых. Исследованы вычислительные свойства сетей клеточных автоматов и обоснована возможность их использования при построении базовых арифметических модулей для криптосистем. Показаны пути и способы повышения надежности арифметических модулей за счет использования встроенных средств диагностики неисправностей в схемах, оперирующих в конечных полях.

По мере технического совершенствования систем защиты информации возникла необходимость в разработке компактных высокоскоростных устройств, способных в режиме реального времени обеспечивать безопасную передачу данных. Надежность любой криптосистемы обеспечивается, во-первых, криптостойкостью реализуемого алгоритма, а, во-вторых, использованием таких арифметических модулей для выполнения основных операций криптоалгоритмов, которые отвечают требованиям контролепригодности и тестопригодности. Существующие архитектуры умножителей в конечных полях направлены на выполнение умножение элементов поля по какому-либо одному методу, а их надежность обеспечивается схемами функцианального диагностирования.

В диссертационной работе получил развитие метод синтеза пословно-последовательных умножителей элементов конечных полей $GF(2^p)$ с блочно-модульной архитектурой на основе использования сетей клеточных автоматов. Показано, что пословно-последовательная архитектура отвечает наилучшему соотношению аппаратных и временных затрат. Предложен новый метод синтеза логической схемы пословно-последовательного умножителя Монтгомери в конечных полях на основе блочно-модульной архитектуры с учетом реализации синтезированной схемы на ПЛИС типа FPGA.

Обоснована возможность объединения вычислительных способностей умножителя Монтгомери и схемы, выполняющей прямое умножение элементов конечного поля, в одной архитектуре. Впервые предложен декомпозиционный метод и процедура синтеза универсального пословно-последовательного умножителя в полях Галуа $GF(2^p)$ со встроенными средствами тестового диагностирования.

Приведены результаты экспериментальных исследований разработанных архитектур умножителей по аппаратным затратам.

Разработаны методы и процедуры синтеза одноканальных и многоканальных сигнатурных анализаторов на сетях клеточных автоматов, основанные на эквивалентности характеристических матриц сетей клеточных автоматов и сдвиговых регистров с линейными обратными связями. Впервые предложен метод синтеза генераторов тестовых последовательностей на сетях клеточных автоматов, который позволяет исключить использование базы

тестовых данных на запоминающих устройствах и упростить аппаратную реализацию генераторов тестов на ПЛИС.

Ключевые слова: компьютерные системы и сети, сети клеточных автоматов, система защиты информации, умножение в конечных полях, пословно-последовательная архитектура, тестовое диагностирование, сигнатурный анализатор.

Gormakova I.V. Synthesis methods of arithmetic units with embedded diagnostic infrastructure for information protection system. – Manuscript.

Thesis for a Candidate Degree in Technical Sciences: Specialty 05.13.05 – computer system and components. – National Technical University «Kharkiv Politechnic Institute», Kharkov 2013.

The thesis is devoted to developing methods and synthesis procedures of universal multipliers based on FPGA with embedded diagnostic infrastructure to perform multiplication of finite field $GF(2^p)$ elements.

Algorithms and methods of multiplication finite field $GF(2^p)$ elements are investigated. The thesis reveals computational properties of cellular automata and substantiates a possibility of their application to produce basic arithmetic units for cryptosystem. The thesis substantiates the application of a word-serial architecture for hardware implementations because of the good scalability between speed and hardware size.

The synthesis method of logic sheme for word-serial finite field $GF(2^p)$ Montgomery multiplier based on block-unit architecture using cellular automata is proposed. The decomposition method and synthesis procedure of universal word-serial finite field $GF(2^p)$ multiplier with built-in test diagnostics means are suggested. The obtained in result architecture combines computational properties of both word-serial finite field multiplier and word-serial finite field Montgomery multiplier.

Experimental results of proposed finite field multiplier architectures in terms of hardware costs are given.

Methods and synthesis procedures of one-demention single input and multiple input cellular automata-based signature analyzers are developed. These methods are based on the equivalence of both characteristic matrices of a cellular automata network and a linear feedback shift register.

Synthesis methods of cellular automata-based test generators wich allow to exclude using of test database on memory and simplify a hardware implementation on VLSI are suggested.

Key words: computer system and network, cellular automata network, information protection system, finite field multiplication, word-serial architecture, test diagnostics, signature analyzer.

Відповідальний за випуск
к.т.н., доц. кафедри автоматики та управління в технічних системах НТУ "ХПІ"
Гунбін М.В.

Підписано до друку 28.05.2013 р. Формат 60x90 1/16.
Папір офсетний. Друк – ризографія. Гарнітура Times New Roman.
Умовн. друк. арк. 0,9. Наклад 110 прим. Зам. № 124118

Надруковано у ФОП Ізрайлєв Є.М.
Свідоцтво № 24800170000040432 від 21.03.2001р.
61002, м. Харків, вул. Фрунзе, 16