Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U004788

Особливі позначки: відкрита

Дата реєстрації: 18-07-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гормакова Ірина Володимирівна
2. Gormakova Irina Vladimirovna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 02-07-2013

Спеціальність за освітою: 8.05090204

Місце роботи здобувача: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: 61001, м. Харків, вул. Кирпичова, 2

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 64.050.14

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: 61001, м. Харків, вул. Кирпичова, 2

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.09.31

Тема дисертації:

1. Методи синтезу арифметичних модулів із вбудованою діагностичною інфраструктурою для систем захисту інформації

2. Synthesis methods of arithmetic units with embedded diagnostic infrastructure for information protection system

Реферат:

1. Об'єкт дослідження: процеси синтезу та логічного проектування компонентів комп'ютерних систем із вбудованими засобами сигнатурного моніторингу. Мета - 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. Методи дослідження: методи теорії цифрових автоматів, методи теорії графів та алгебри регулярних подій, методи та процедури криптографії, методи технічного діагностування. Теоретичні та практичні результати: розроблено методи та процедури синтезу універсальних помножувачів в полях GF(2p) на ПЛІС

типу FPGA, підвищено достовірність їх функціонування за рахунок включення до схеми помножувача вбудованих засобів тестового діагностування. Наукова новизна: вперше розроблена автоматна модель клітинного автомата на базі алгебри регулярних подій; розроблено метод синтезу генераторів детермінованих тестових послідовностей на мережах клітинних автоматів; розроблено метод синтезу логічної схеми модуля множення Монтгомері в скінченних полях; отримали подальший розвиток матричні моделі мереж клітинних автоматів, методи синтезу послівно-послідовних помножувачів в скінченних полях Галуа, методи синтезу універсальних послівно-послідовних помножувачів в полях Галуа із вбудованими генераторами тестових послідовностей. Впровадження: результати впроваджені у ДП "Харківський науково-дослідний інститут комплексної автоматизації" (м. Харків), Національний технічний університет "ХПІ" (м. Харків). Сфера використання: програмно-апаратні засоби управління складними об'єктами на ПЛІС. (див. продовження)

2. The object of study: the processes of synthesis and component logic design for computer systems with embedded signature monitoring instruments. The aim of the study - to increase the level of controllability and reduce diagnosing complexity of arithmetic modules for cryptographic systems through the development of models, methods and synthesis procedures of digital devices with built-in diagnostic infrastructure signature monitoring to be implemented using modern components. Methods: methods of digital automata theory, graph theory and algebra of regular events, methods and procedures of cryptography, methods of technical diagnostics. Theoretical and practical results: the methods and synthesis procedures of universal field GF(2p) multipliers on PLD type FPGA are developed, the accuracy of their operation on account of including built-in diagnostic test instruments in multiplier circuit is increased. Scientific novelty: first cellular automaton model on the basis of the regular events algebra is developed, the synthesis method of deterministic test pattern generator on the cellular automata, the synthesis method of logic scheme of Montgomery multiplication unite in finite fields is developed, further developed the matrix models of cellular automata, synthesis methods word-serial multiplier architectures in finite Galois fields, synthesis methods of the universal word-serial multipliers in Galois fields with built-in test pattern generators. Degree of implementation: results implemented in SE "Kharkov Research Institute of Integrated Automation" (Kharkov), National technical university "Kharkov polytechnic institute" (Kharkov). Application area: software-hardware devices for complex objects control on the PLD.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Дербунович Леонід Вікторович

2. Derbunovich Leonid Victorovich

Кваліфікація: д.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кривуля Геннадій Федорович
2. Кривуля Геннадій Федорович

Кваліфікація: д.т.н., 01.05.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кошман Сергій Олександрович
2. Кошман Сергій Олександрович

Кваліфікація: к.т.н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Качанов Петро Олексійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Качанов Петро Олексійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.