

АНОТАЦІЯ

Кирилюк Т. П. Синтез відмовостійких зворотних логічних пристроїв методами штучного інтелекту. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 121 – «Інженерія програмного забезпечення» – Чернівецький національний університет імені Юрія Федьковича, Чернівці, 2026.

Дисертаційна робота присвячена вирішенню науково-прикладної задачі підвищення ефективності автоматизованого проєктування зворотних та квантових логічних схем з використанням методів штучного інтелекту, зокрема розробці інформаційної технології для структурного синтезу відмовостійких пристроїв, які характеризуються мінімальною квантовою вартістю та здатністю до збереження парності сигналів на базі узагальнених вентилів Фредкіна. Також вивчено та вдосконалено моделі еволюційного пошуку, які завдяки використанню об'єктно-орієнтованого представлення хромосом та адаптивних операторів мутації є основним алгоритмічним інструментом при генерації оптимальної топології схеми великої розмірності.

Результати роботи є підґрунтям для подальших теоретичних і практичних наукових розробок у галузі автоматизації проєктування квантових обчислювачів та криптографічних систем на їх основі.

Дисертація складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел та додатків. У **вступі** обґрунтовано актуальність теми дослідження, сформульовано мету, завдання, предмет, об'єкт та методи дослідження, вказано наукову новизну, теоретичне та практичне значення отриманих результатів, подано та проаналізовано зв'язок роботи з науковими темами. Зазначено особистий внесок здобувача, а також наведено відомості про апробацію та публікації основних результатів дисертації. Описано структуру та обсяг дисертаційної роботи.

Перший розділ містить ключові відомості з теорії зворотної логіки, опис основних напрямів досліджень та завдання, якими займається сучасна інженерія квантових зворотних схем. Тут проведено огляд та опис існуючих підходів до синтезу (детерміновані алгоритми, класичні еволюційні стратегії), виявлено їхні обмеження, пов'язані з експоненційним зростанням обчислювальної складності. Розглянуто та проаналізовано базові логічні елементи: вентилі Фейнмана, Тоффолі, які є основою для побудови енергоефективних обчислювачів, та їх особливості в контексті відмовостійкості. Okремо описано перевагу вентиля Фредкіна через його унікальну топологію яка забезпечує ефект збереження парності сигналів. Здійснено класифікацію та огляд методів однієї з важливих технік штучного інтелекту – еволюційних обчислень, та обґрунтовано доцільність використання генетичних алгоритмів для вирішення багатокритеріальних оптимізаційних задач синтезу.

У другому розділі систематизовано теоретичні засади проєктування зворотних схем та проведено класифікацію логічних вентилів, від класичних бінарних до квантових вентилів. Розглянуто матричне представлення логічних елементів, що дозволило формалізувати процеси перетворення інформації у векторному просторі станів. Проаналізовано умови функціональної повноти для універсальних базисів, що є необхідною умовою для синтезу довільної булевої функції. Визначено ключові критерії якості синтезованих рішень: квантову вартість, глибину схеми та апаратну складність. Okрему увагу приділено проблемі надлишковості виходів та питанням відмовостійкості, зокрема методам збереження парності сигналів для забезпечення надійності обчислень. Здійснено огляд існуючих метаевристичних підходів до синтезу, таких як метод симульованого відпалу, алгоритми мурашиних колоній та класичні генетичні алгоритми. Виявлено їхні спільні недоліки: схильність до передчасної збіжності,

застрягання в локальних екстремумах та низьку ефективність при роботі зі схемами великої розмірності.

Основні результати даного розділу можна підсумувати наступним чином:

- формалізовано математичний апарат зворотної логіки для подальшої автоматизації синтезу;

- обґрунтовано вибір метрик оптимізації, які враховують як мінімізацію ресурсів, так і вимоги до відмовостійкості;

- на основі порівняльного аналізу доведено необхідність розробки вдосконаленого генетичного методу, здатного подолати обмеження існуючих аналогів.

Третій розділ присвячений розробці та програмній реалізації вдосконаленого генетичного методу структурного синтезу зворотних схем. Особливу увагу приділено розширенню бази шляхом синтезу нових реконфігурованих пристроїв на основі узагальненого вентиля Фредкіна. Використання таких вентилів дозволяє створювати схеми з внутрішньою апаратною відмовостійкістю, завдяки збереженню парності сигналів між входами та виходами, що є сильною стороною запропонованого підходу. Детально описано запроповану модифікацію алгоритму, яка, на відміну від класичних підходів, використовує об'єктно-орієнтовану модель представлення хромосом. Це дозволило перейти від «сліпої» оптимізації бітових масивів до оперування функціональними об'єктами вентилів і схем з визначеними властивостями, що суттєво зменшує простір пошуку рішень. Розроблено та обґрунтовано комплексний оператор багатокomпонентної мутації, який інтегрує три типи структурних змін: додавання, видалення, та модифікація параметрів та забезпечує баланс між дослідженням простору рішень та експлуатацією знайдених оптимумів. Для вирішення проблеми маршрутизації сигналів впроваджено механізм динамічної перестановки вихідних ліній, що дозволяє алгоритму ефективно виходити з локальних

екстремумів. Окрему увагу приділено програмній реалізації методу. Описано архітектуру розробленого програмного комплексу мовою C#, який здійснює повний цикл синтезу. Реалізовано модуль автоматичної трансляції схем у формат OpenQASM, що забезпечило пряму сумісність із квантовим фреймворком IBM Qiskit для верифікації результатів.

Основні результати даного розділу можна підсумувати наступним чином:

- запропоновано розширений базис на основі реконфігурованих узагальнених вентилів Фредкіна, що забезпечує апаратну відмовостійкість синтезованих схем;
- розроблено вдосконалений генетичний метод із використанням об'єктно-орієнтованої моделі хромосоми;
- реалізовано адаптивні еволюційні оператори для оптимізації топології та маршрутизації зворотних схем;
- створено автоматизовану систему синтезу зворотних пристроїв, інтегровану з сучасними засобами квантового моделювання.

У **четвертому розділі** наведено результати експериментальних досліджень та практичної апробації розробленого математичного і програмного забезпечення. Здійснено синтез еталонних тестових наборів зворотних функцій різної розмірності та проведено порівняльний аналіз отриманих схем з результатами роботи відомих аналогів. Статистичний аналіз підтвердив, що запропонований вдосконалений генетичний метод дозволяє зменшити квантову вартість схем при збереженні прийнятної часу генерації. Особливу увагу приділено практичному застосуванню розробленої технології. Описано процес синтезу відмовостійкого зворотного потокового шифратора на базі реконфігурованих елементів RRG2 та RRG3 та його подальшу апаратну реалізацію на базі FPGA сімейства Altera Cyclone IV. Для верифікації проєкту застосовано метод вичерпного

тестування, який підтвердив повну функціональну еквівалентність синтезованої схеми вихідній специфікації.

Основні результати даного розділу можна підсумувати наступним чином:

- експериментально підтверджено ефективність розробленого методу на стандартних наборах тестових функцій;

- здійснено успішну апаратну імплементацію синтезованого криптографічного пристрою з підтверженою відмовостійкістю, досягнуто високих показників швидкодії (максимальна частота $F_{max} \approx 310$ МГц);

- доведено придатність розроблених засобів для автоматизованого проєктування високопродуктивних компонентів систем на кристалі.

У **висновках** підсумовано основні теоретичні та практичні результати дисертаційного дослідження, які в сукупності вирішують актуальну науково-прикладну задачу підвищення ефективності синтезу зворотних відмовостійких логічних пристроїв.

У **додатках** подано наукові публікації, в яких відображено основні результати роботи, відомості про апробацію – акти про впровадження результатів дослідження, лістинги ключових модулів розробленого програмного забезпечення, приклади синтезованих схем у форматі OpenQASM та фрагменти Verilog-коду для FPGA.

Теоретичне значення. Результати теоретичних досліджень, а саме розроблена математична модель структурного синтезу, розширений базис реконфігурованих вентилів Фредкіна та модифікований генетичний метод з об'єктно-орієнтованою хромосомою, поглиблюють теорію проєктування квантових обчислювачів. Вони можуть використовуватися для подальших наукових досліджень у галузі автоматизації проєктування, а також у навчальних курсах кафедр програмного забезпечення комп'ютерних систем та комп'ютерних систем та мереж Чернівецького національного

університету імені Юрія Федьковича, пов'язаних з теорією алгоритмів, архітектурою комп'ютерних систем та квантовими обчисленнями.

Практичне значення. Розроблений у дисертаційній роботі програмний комплекс автоматизованого синтезу, модуль трансляції схем у формат OpenQASM та реалізований на FPGA відмовостійкий зворотний шифратор на базі узагальнених вентилів Фредкіна можуть в подальшому використовуватися для створення енергоефективних компонентів систем на кристалі. Запропоновані підходи до інтеграції з IBM Qiskit дозволяють верифікувати складні квантові алгоритми.

Ключові слова: оптимізація, програмне забезпечення, продуктивність, інформаційна система/інформаційні технології, модель, відмовостійкість, автоматизація, моделювання, генетичний алгоритм, швидка еволюція, машинне навчання, інтелектуальна система, мутація параметрів, штучний інтелект, алгоритм.

ABSTRACT

Kyrylyuk T. Synthesis of fault-tolerant reversible logic devices using artificial intelligence methods. – Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 121 – “Software Engineering” – Yuriy Fedkovych Chernivtsi National University, Chernivtsi, 2026.

The dissertation is devoted to solving the scientific and applied problem of increasing the efficiency of automated design of reversible and quantum logic circuits using artificial intelligence methods, in particular, the development of information technology for the structural synthesis of fault-tolerant devices, which are characterized by minimal quantum cost and the ability to preserve signal parity based on generalized Fredkin gates. Evolutionary search models have also been studied and improved, which, thanks to the use of object-oriented representation of chromosomes and adaptive mutation operators, are the main algorithmic tool in generating the optimal topology of a high-dimensional circuit.

The results of the work are the basis for further theoretical and practical scientific developments in the field of automation of the design of quantum computers and cryptographic systems based on them.

The dissertation consists of an introduction, four sections, conclusions, a list of sources used and appendices. The **introduction** substantiates the relevance of the research topic, formulates the goal, objectives, subject, object and methods of the research, indicates the scientific novelty, theoretical and practical significance of the results obtained, presents and analyzes the connection of the work with scientific topics. The personal contribution of the applicant is indicated, and information about the testing and publication of the main results of the dissertation is provided. The structure and scope of the dissertation work are described.

The **first chapter** contains key information on the theory of reversible logic, a description of the main areas of research and the tasks that modern quantum reversible circuit engineering deals with. Here, a review and description of existing approaches to synthesis (deterministic algorithms, classical evolutionary strategies) are conducted, their limitations associated with the exponential growth of computational complexity are identified. The basic logical elements are considered and analyzed: Feynman and Toffoli gates, which are the basis for building energy-efficient computers, and their features in the context of fault tolerance. The advantage of the Fredkin gate due to its unique topology that provides the effect of preserving signal parity is separately described. The methods of one of the important techniques of artificial intelligence - evolutionary computing - are classified and reviewed, and the feasibility of using genetic algorithms for solving multi-criteria optimization problems of synthesis is substantiated.

In the **second chapter**, the theoretical principles of designing reversible circuits are systematized and a classification of logic gates is carried out, from classical binary to quantum gates. The matrix representation of logic elements is considered, which allowed formalizing the processes of information transformation in the vector space of states. The conditions of functional completeness for universal bases, which is a

necessary condition for the synthesis of an arbitrary Boolean function, are analyzed. The key criteria for the quality of synthesized solutions are determined: quantum cost, circuit depth, and hardware complexity. Special attention is paid to the problem of output redundancy and fault tolerance issues, in particular, methods for preserving signal parity to ensure the reliability of calculations. A review of existing metaheuristic approaches to synthesis, such as the simulated annealing method, ant colony algorithms, and classical genetic algorithms, is carried out. Their common shortcomings are identified: a tendency to premature convergence, getting stuck in local extrema, and low efficiency when working with high-dimensional circuits.

The main results of this section can be summarized as follows:

- the mathematical apparatus of reversible logic is formalized for further automation of synthesis;
- the choice of optimization metrics is justified, which take into account both resource minimization and fault tolerance requirements;
- based on a comparative analysis, the need to develop an improved genetic method capable of overcoming the limitations of existing analogues is proven.

The **third chapter** is devoted to the development and software implementation of an improved genetic method for structural synthesis of reversible circuits. Particular attention is paid to expanding the base by synthesizing new reconfigurable devices based on the generalized Fredkin gate. The use of such gates allows creating circuits with internal hardware fault tolerance, due to the preservation of signal parity between inputs and outputs, which is a strong point of the proposed approach. The proposed modification of the algorithm is described in detail, which, unlike classical approaches, uses an object-oriented model of chromosome representation. This allowed us to move from "blind" optimization of bit arrays to operating on functional objects of gates and circuits with defined properties, which significantly reduces the solution search space. A complex multicomponent mutation operator has been developed and substantiated, which integrates three types of structural changes: addition, deletion, and modification of parameters and provides a balance between exploring the solution space and

exploiting the found optima. To solve the signal routing problem, a mechanism for dynamic permutation of output lines has been introduced, which allows the algorithm to effectively exit local extrema. Special attention is paid to the software implementation of the method. The architecture of the developed software complex in C#, which performs a full synthesis cycle, is described. A module for automatic translation of schemes into the OpenQASM format has been implemented, which provided direct compatibility with the IBM Qiskit quantum framework for verifying results.

The main results of this section can be summarized as follows:

- an extended basis based on reconfigured generalized Fredkin gates has been proposed, which provides hardware fault tolerance of synthesized schemes;
- an improved genetic method has been developed using an object-oriented chromosome model;
- adaptive evolutionary operators are implemented to optimize the topology and routing of reversible circuits;
- an automated system for the synthesis of reversible devices is created, integrated with modern quantum modeling tools.

The **fourth chapter** presents the results of experimental research and practical testing of the developed mathematical and software. The synthesis of reference test sets of reversible functions of various dimensions is carried out and a comparative analysis of the obtained circuits with the results of the work of known analogues is carried out. Statistical analysis confirmed that the proposed improved genetic method allows to reduce the quantum cost of circuits while maintaining an acceptable generation time. Special attention is paid to the practical application of the developed technology. The process of synthesizing a fault-tolerant reversible stream encoder based on reconfigurable elements RRG2 and RRG3 and its subsequent hardware implementation based on the FPGA of the Altera Cyclone IV family is described. The exhaustive testing method was used to verify the project, which confirmed the full functional equivalence of the synthesized circuit to the original specification.

The main results of this section can be summarized as follows:

- the effectiveness of the developed method was experimentally confirmed on standard sets of test functions;
- a successful hardware implementation of a synthesized cryptographic device with confirmed fault tolerance was carried out, high performance indicators were achieved (maximum frequency $F_{max} \approx 310$ MHz);
- the suitability of the developed tools for automated design of high-performance components of systems on a crystal was proven.

The **conclusions** summarize the main theoretical and practical results of the dissertation research, which together solve the current scientific and applied problem of increasing the efficiency of synthesis of reversible fault-tolerant logic devices.

The **appendices** contain scientific publications that reflect the main results of the work, information on testing - acts on the implementation of the research results, listings of key modules of the developed software, examples of synthesized circuits in OpenQASM format and fragments of Verilog code for FPGA.

Theoretical significance. The results of theoretical research, namely the developed mathematical model of structural synthesis, the extended basis of reconfigurable Fredkin gates and the modified genetic method with an object-oriented chromosome, deepen the theory of quantum computer design. They can be used for further scientific research in the field of design automation, as well as in training courses of the departments of computer systems software and computer systems and networks of Yuriy Fedkovych Chernivtsi National University related to the theory of algorithms, architecture of computer systems and quantum computing.

Practical significance. The software complex of automated synthesis developed in the dissertation work, the module for translating schemes into the OpenQASM format and the fault-tolerant reversible encoder based on generalized Fredkin gates implemented on FPGA can be further used to create energy-efficient components of systems-on-Chip. The proposed approaches to integration with IBM Qiskit allow for the verification of complex quantum algorithms.

Keywords: optimization, software, performance, information system/information technology, model, fault tolerance, automation, modeling, genetic algorithm, rapid evolution, machine learning, intelligent system, parameter mutation, artificial intelligence, algorithm.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці у виданнях, включених до переліку наукових фахових видань України та проіндексованих у наукометричних базах даних Web of Science Core Collection та/або Scopus:

1. Kyryliuk T., Palahuta M., Deibuk V. Using artificial intelligence methods for the optimal synthesis of reversible networks. *Radioelectronic and Computer Systems*. 2024. Vol. 2024, no. 4. P. 112–122. URL: <https://doi.org/10.32620/reks.2024.4.10> (Scopus, Q3)

Внесок авторів: **Кирилюк Т.** – розроблення алгоритму, проведення експериментів, підготовка основного рукопису; **Палагута М.** – розроблення алгоритму, проведення експериментів, підготовка основного рукопису; **Дейбук В.** – рецензування та редагування рукопису.

Наукові праці у виданнях, проіндексованих у наукометричній базі даних Scopus:

2. Deibuk V., Dovhaniuk O., Kyryliuk T. The Extended Fredkin Gates with Reconfiguration in NCT Basis. *Lecture Notes on Data Engineering and Communications Technologies*. 2023. Vol. 181 : Advances in Computer Science for Engineering and Education VI : ICCSEEA 2023 (Warsaw, Poland, 17–19 March 2023). Warsaw, P. 95–105. URL: https://doi.org/10.1007/978-3-031-36118-0_9. (Scopus)

Внесок авторів **Дейбук В.** – наукове керівництво, концептуальна перевірка, рецензування та редагування рукопису; **Довганюк О.** – написання рукопису,

проведення експериментів та аналіз результатів; **Кирилюк Т.** – проведення експериментів, перевірка результатів та доопрацювання рукопису

3. Dovhaniuk O., Kyryliuk T., Deibuk V. Reversible Fault-Tolerant Encryption Using Extended Fredkin Gate with Reconfiguration. *Advances in Transdisciplinary Engineering*. 2025. Vol. 65 : Artificial Intelligence, Medical Engineering and Education : AIMEE 2024 (Huangshi, China, 26–27 Oct. 2024). Huangshi, P. 69–76. DOI: <https://doi.org/10.3233/atde250113>. (Scopus).

Внесок авторів: Довганюк О. – проведення експериментів; **Кирилюк Т.** – основне написання рукопису, верифікація експериментів, підготовка презентації; Дейбук В. – рецензування рукопису та наукове керівництво.

Наукові праці, які засвідчують апробацію матеріалів дисертації;

4. Kyryliuk T., Deibuk V., Kyryliuk S. Synthesis of reversible circuits by genetic algorithm with multicomponent mutation. *Інформаційні технології та комп'ютерне моделювання* : матеріали міжнар. наук.-практ. конф. (м. Івано-Франківськ, 6–8 лип. 2023 р.). Івано-Франківськ, 2023. С. 150–151.

Внесок авторів: **Кирилюк Т.** – проведення експериментів, розроблення алгоритму, підготовка основного рукопису; Дейбук В. – наукове керівництво, доопрацювання рукопису; Кирилюк С. – проведення експериментів, фіксація експериментальних результатів