

01.09.2022

01.09.2022



РЕЦЕНЗИЯ

на дисертационен труд
за придобиване на образователна и научна степен „Доктор“
по професионално направление 5.3 Комуникационна и
компютърна техника,
научна специалност „Автоматизация на инженерния труд и
системи за автоматизация на проектирането”

Автор на дисертационния труд:

Ериселда Малай

Тема на дисертационния труд: „Разработване на нови
хардуерни решения за киберсигурност на комуникационни системи”
доц. д-р инж. Тихомир Брусев,
Технически Университет - София

1. Актуалност на разработвания в дисертационния труд проблем в научно и научноприложно отношение. Степен и нива на актуалността на проблема и конкретните задачи, разработени в дисертацията.

В наши дни голям брой електронни устройства са свързани помежду си и предават големи количества данни с висока скорост, използвайки съвременни технологии като изкуствен интелект, интернет на нещата и 5G. От друга страна, рисковете за киберсигурността се увеличават. Хардуерно-базираното логическо криптиране предлага силна защита на ниво схема. Стандартната софтуерно-базирана защита е уязвима към атаки със съвременни инструменти за обратно инженерство. Полупроводниковата индустрия е изложена на големи рискове поради глобализацията на проектирането на интегрални схеми, което води до заплахи като кражба на интелектуална собственост, свръхпроизводство и хардуерна манипулация. Важно да се разработват нови хардуерни решения за киберсигурност на комуникационните системи, за да се защитят съвременните системи от усъвършенствани атаки.

Логическото криптиране може да помогне за защитата на интелектуалната собственост и на интегралните схеми (ИС) срещу обратно инженерство и хардуерна манипулация. Предназначението на тази техника е да подобри сигурността на цифровите схеми чрез

вграждане на механизми за криптиране в техните логически елементи. Съществуват редица предизвикателства пред логическото криптиране, като: ефективното интегриране на логическото криптиране в процеса на проектирането, без да се компрометира производителността или функционалността на цифровите схеми; повишаването на устойчивостта на този метод срещу усъвършенствани атаки; правилното управление на ключовете за криптиране за по-добра сигурност; минимизирането на въздействието върху площта на схемата, консумацията на мощност и скоростта.

Основната цел на тази дисертация е да предложи алгоритъм за логическо криптиране, който да постигне надеждна защита на цифровите схеми чрез директно включване на криптирането в логическата структура на схемата.

За постигане на тази цел докторантката е формулирала задачи, свързани с разработването на методология за оценка на ефективността на техниките за хардуерно криптиране в комуникационните системи. Дефинирани са ограниченията в производителността на настоящите подходи за хардуерно криптиране в комуникационните схеми. Оценени са различни техники за криптиране на логическо ниво по отношение на площ, времезакъснения и енергийни разходи. Определена е техниката, която предлага най-добрия компромис между силата на криптиране и хардуерната ефективност. Предложените в тази дисертация решения са валидирани на практика.

Изследванията в дисертацията са насочени към разработване на ефикасни методи за логическото криптиране на цифрови схеми, подобряване на устойчивостта срещу различни атаки и установяване на надеждни практики за управление на ключове. Усилията са фокусирани върху усъвършенстване на съвременната хардуерна защита и предоставяне на практически решения за защита на интегрални схеми от нововъзникващи заплахи. За тази цел се използва комбинация от теоретичен анализ, симулации и емпирични валидации. Дефинирана е техника за криптиране, която осигурява най-силна обфускация.

Всичко това определя актуалността на изследвания проблем, както от научноприложна, така и от приложна гледни точки.

2. Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал.

В тази дисертация са използвани 200 литературни източника. Повечето от тях са от последните 10 години. Това ми дава основание да смятам, че докторантката Ериселда Малай познава съвременното състояние на решаваните от него проблеми, което е основа за успешно решаване на поставените задачи.

3. Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд.

Докторантката Ериселда Малай е формулирала цел и задачи, които са адекватни и съответстват на изискванията за дисертационен труд за придобиване на образователната и научна степен „Доктор“.

Литературното проучване показва редица предизвикателства и пропуски в областта на логическото криптиране, които са свързани с: устойчивост срещу нови усъвършенствани методи атаки, като тези, произтичащи от напредъка в квантовите изчисления; предизвикателства при управлението на ключове и необходимостта от по-ефективни и мащабируеми механизми за криптиране.

Избраната методика комбинира теоретичен анализ, проектиране на хардуер, оценка базирана на симулация и оценка на сигурността. Основният фокус е насочен върху разработването и оценяването на техники за криптиране на логическо ниво, които подобряват сигурността на схемите, като същевременно поддържат приемливи разходи за проектиране. Цялостният подход включва следните фази: проектиране и интегриране на логическо криптиране; описание и внедряване на хардуера; оценка на производителността; оценка на сигурността; сравнителен анализ и валидиране. Самото логическо криптиране включва три различни методологии за събиране на данни, а именно експериментален подход, подход базиран на симулация и подход за оценка и валидиране.

4. Кратка аналитична характеристика на естеството и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд.

Представената дисертация се състои от 165 страници текст и 153 страници приложения, много добре структурирани в пет глави, списък на публикациите, списък на цитираните статии, списък на фигури и таблици, списък на съкращенията, увод, ограничения, бъдеща работа, приноси и изпозвана литература.

В глава I е направен литературен обзор. Представен е преглед на въпросите свързани с киберсигурността в комуникационните системи. Анализирани са методът за хардуерна обфускация. Извършено е описание на обфускацията на ниво Register Transfer Level (RTL), на обфускацията на логическо ниво, на обфускацията на ниво топология, на обфускацията на ниво инструкции и на обфускацията на ниво печатни платки. Разгледан е процесът на криптиране на логиката на при хардуерното проектиране. Направено е сравнение между подходите за хардуерна и софтуерна защита. Разгледани са проблемите свързани със сигурността и уязвимостта в процеса на проектиране на интегралните схеми. Изброени са различните видове хардуерни атаки. Обяснено е естеството и рисковете, свързани с атаките с хардуерни троянски коне, както и таксономията на хардуерните троянски коне. Описани са различни видове атаки, като например атаки свързани с обратното инженерство, атаки през странични канали, атаки за анализ на мощността, атаки с инжектиране на грешки. Класифицирани и сравнени са различни видове криптографски алгоритми, внедрени в хардуерните устройства. Представени са предизвикателствата пред хардуерната сигурност, както и инструментите и техниките за защита на хардуерните устройства. Разгледани са най-широко използваните техники за логическо криптиране – криптиране чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ(XOR/XNOR), криптиране чрез използване на мултиплексори (MUX) и криптиране чрез използване на тригери (Flip-Flop).

Методите за изследване на хардуерното криптиране са представени в Глава II. Възприета е многоетапна методология за изследване на ефективната интеграция и надеждността на сигурността. Основният фокус е върху разработването и оценката на техники за криптиране на логическо ниво, които подобряват сигурността на схемите, като същевременно поддържат приемливи разходи за проектиране. Анализирани са факторите, влияещи върху

логическото криптиране в FPGA проекти. Разработени са различни архитектури за логическо криптиране. Описани са техниките за логическо криптиране чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ, чрез използване на мултиплексори (MUX) и чрез използване на тригери. Представена е последователността на хардуерната реализация на логическото криптиране за FPGA проекти. Ефективността на техниките за логическо криптиране се оценява с помощта на комбинация от показатели за хардуерна производителност и сигурност. Стратегиите за управление на ключове се анализират по отношение на сигурното съхранение, контролираното активиране, мащабируемостта, разпределението и чувствителността към ключовете. Проведен е сравнителен анализ на всички предложени техники за логическо криптиране, използвайки унифициран набор от показатели за производителност и сигурност.

В Глава III е представено внедряването и систематичната оценка на техниките за хардуерно криптиране на логиката за подобряване на киберсигурността на комуникационните системи. Изследвани са три механизма за криптиране: чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ, мултиплексорно-базирано логическо криптиране и тригерно-базирано криптиране. Предложена е алгоритмична рамка за оценка, която количествено оценява устойчивостта на криптирането и разходите за внедряване. Тя интегрира логическата обфускация, ключово-зависимите трансформации и криптирането, за да се направи оценка на сигурността чрез експерименти с инжектиране на грешки, анализ на разстоянието на Хеминг и показателите за разпространение на грешки. Анализирани са въздействията на криптирането върху времезакъсненията, консумацията на мощност и увеличаването на площта на схемите. Предложените техники за криптиране се оценяват с помощта на стандартни ISCAS схеми. Получените резултати показват, че когато се изисква високо ниво на сигурност, алгоритъмът дава приоритет на тригерно-базираното криптиране.

В Глава IV е създаден и представен експериментален тестов стенд за изследване на схеми при използване на различни видове криптиране, базирани на: криптиране чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ, мултиплексорно-базирано логическо криптиране и тригерно-базирано криптиране.

Изследването има за цел да тества и анализира разстоянията на Хеминг, при използването на неправилни ключове за активиране и генериране на неправилен и правилен изходен сигнал. Логическите схеми са описани на езика VHDL. Анализирани са три вида логически техники за криптиране, базирани на криптиране чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ, мултиплексорно-базирано логическо криптиране и тригерно-базирано криптиране.

В Глава V са представени симулационни изследвания и оценка на различни хардуерни решения за киберсигурност на комуникационни системи. Обобщени са получените резултати за средното разстояние на Хеминг (AHD) и средната чувствителност на грешки (AFS) за всяка ISCAS схема. Получените резултати показват, че тригерно-базирано криптиране постига най-високото AHD и най-ниското AFS при изследваните схеми. Направените заключения показват, че криптирането чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ осигурява най-ниска защита от атаки, но при него има най-малко увеличаване на площта на схемите в следствие на добавените логически елементи. При тригерно-базирано криптиране се постига най-добра защита на цифровите схеми, за сметка на увеличана консумация на мощност и значително нарастване на общата площ на схемите. Криптирането чрез използване на мултиплексори заема средно място между гореспоменатите видове криптирания по отношение на ниво на защита, увеличана площ на цифровите схеми и енергийни разходи.

5. Научни, научноприложни и приложни приноси на дисертационния труд.

В докторската дисертация авторът е посочил 8 приноса. Четири от тях са научен, два са научно-приложни и два са приложни. Приемам приносите, формулирани от докторантката Ериселда Малай, които могат да бъдат обобщени по следния начин:

- Разработен е алгоритъм за количествена оценка на логическо криптиране на цифрови схеми.
- Предложена е количествена мярка за оценка, която интегрира различни показатели характеризиращи сигурността на системите. По този начин може да се направи сравнение

между различните методи на логическо криптиране, използвани за защита на цифрови схеми.

- Получените експерименталните резултати потвърждават, че тригерно-базирано криптиране осигурява на добра защита от различни видове атаки, като инжектиране на грешки и SAT-базирани атаки.
- Предложен е прагов алгоритъм за преобразуване на експериментални показатели за сигурност в детерминистични решения, за внедряване на логическо криптиране с различни степени на защита. На базата на този алгоритъм се дефинира подходящо приложение на логическото криптиране и се препоръчват платформи за внедряване, като програмируема логика (FPGA) и специализирани интегрални схеми (ASIC).
- Направен е сравнителен анализ на различни техники за логическо криптиране, като криптиране чрез използване на логически елементи изключващо ИЛИ/изключващо ИЛИ-НЕ, криптиране чрез използване на мултиплексори и криптиране чрез използване на тригери.
- Анализирано е влиянието на броя на използваните логически елементи при криптирането върху степента на защита на схемите и разходите за внедряване.
- Предложеният алгоритъм в дисертационния труд, както и различните анализирани техники за логическо криптиране са валидирани на практиката, като са направени изследвания използвайки схемите ISCAS-85 и ISCAS-89.

Смятам, че получените резултати са оригинални и изцяло съответстват на изискванията за дисертационен труд за придобиване на образователната и научна степен „Доктор“.

6. Оценка за степента на личното участие на дисертанта в приносите.

За личните приноси на докторантката Ериселда Малай съдя от факта, че тя има един самостоятелен научен труд, а в осем от останалите тя е първи съавтор. Това ми дава основание да приема, че дисертационният труд и приносите са лично дело на кандидата.

7. Преценка на публикациите по дисертационния труд. Отражение в науката.

По дисертацията са направени девет публикации. Три от докладите са докладвани на конференция в България. Осем от статиите са реферирани в Scopus. Докторантката е съавтор на глава от книга, цитирана в Scopus.

Направените публикации надхвърлят минималните изисквания за присъждане на образователната и научна степен „Доктор“. Приемам, че основните резултати на дисертационния труд са достойни на международната и българската научна общественост.

8. Използване на резултатите от дисертационния труд в научната и социалната практика.

Много положителен е фактът, че реализираните изследвания на докторантката са проведени в рамките на Съвместната докторска програма в мрежата CEEPUS номер: CIII-BG-1103-06-2122.

9. Оценка на съответствието на автореферата с изискванията за изготвянето му, както и на адекватността на отразяване на основните положения и приносите на дисертационния труд.

Авторефератът напълно отразява съдържанието и получените резултати в дисертационния труд, като са подчертани основните приноси. Също така изцяло са спазени изискванията за изготвяне на авторефератите в Техническия университет – София, поради което дадох и положителен отзив за неговото отпечатване.

10. Мнения, препоръки и бележки.

Всички препоръки и забележки, направени от мен в предварителното мнение, както и на предварителното обсъждане на дисертационния труд са изпълнени.

11. Заключение с ясна положителна или отрицателна оценка на дисертационния труд.

Считам, че дисертационният труд „Разработване на нови хардуерни решения за киберсигурност на комуникационни системи“ на докторантката Ериселда Малай покрива изискванията на Закона за развитие на академичния състав в Република България и

Правилника за неговото приложение. Приемам че, направените изводи и заключения са логически и компетентно построени.

Въз основа на получените научни, научноприложни и приложни приноси в дисертацията, демонстрираните образователно ниво и натрупания теоретичен и практически опит, значимите публикации по дисертацията, предлагам на научното жури да присъди на Ериселда Малай научната степен „Доктор“ по професионално направление 5.3. Комуникационна и компютърна техника, научна специалност „Автоматизация на инженерния труд и системи за автоматизация на проектирането“.

24. 08. 2026 г.

Изготвил:

(доц. д-р Тихомир Брусев)

DTK 48-HC1-099

01.09.2026

REVIEW

of doctoral thesis
for obtaining the educational and scientific degree "Doctor"
in a professional field

**5.3 Communication and Computer Engineering,
in the scientific specialty „Computer-aided engineering and
computer-aided design systems"**

Author of doctoral thesis:

Eriselda Malaj

Topic of doctoral thesis: „Development of new hardware solutions
for cybersecurity of communication systems"

Assoc. prof. Dr. Eng. Tihomir Brusev,

Technical University of Sofia

1. Relevance of the problem developed in the doctoral thesis in scientific and applied science. Degree and levels of relevance of the problem and the specific tasks developed in the doctoral thesis.

Today, the big numbers of electronic devices are interconnected and transfer large data with high-speed using modern technologies like AI, IoT, and 5G. On the other hand, the cybersecurity risks are increased. The hardware-based security logic encryption offers strong protection at the circuit level. The standard software-based security is vulnerable to attacks with modern reverse engineering tools. The semiconductor industry is exposed to great risks due to the globalization of IC design, which leads to threats such as IP theft, overproduction, and hardware tampering. It is very important to be developed new hardware solutions for cybersecurity of communication systems in order to prevent modern systems from the advanced attacks.

Logic encryption can help to protect intellectual property and secure integrated circuits (ICs) against reverse engineering and hardware tampering. This technique is designed to improve the security of digital circuits by embedding encryption mechanisms within their logic gates. The challenges remain: effectively integration of logic encryption into the design process without compromising their performance or functionality, increasing the resilience of this method against advanced attacks, proper managing of encryption keys for better security and deployments,

minimizing the impact over the circuit's area, power consumption, and speed.

The main goal of this dissertation is to propose a logical encryption algorithm to achieve robust protection of digital circuits by directly incorporating encryption into the logical structure of the circuit.

To achieve this goal, the doctoral student has formulated tasks connected development of methodology for evaluating the effectiveness of hardware encryption techniques in communication systems. The performance limitations of current hardware encryption approaches in communication circuits are defined. Different logic-level encryption techniques, in terms of area, delay, and power overhead are evaluated. The technique which offers the best trade-off between encryption strength and hardware efficiency is determined. The solutions proposed in this thesis have been practically validated.

The investigations in the dissertation are aimed at developing efficient methods for integrating encryption into logic gates, improving resistance to various attack vectors, and establishing robust key management practices. The efforts of this work are focused on to advance the state of the art in hardware security and provide practical solutions for protecting integrated circuits from emerging threats. For this purpose a combination of theoretical analysis, simulation, and empirical validation are used. The encryption technique that provides the strongest obfuscation and key dependency is identified.

All this determines the relevance and significance of the researched problem and the tasks set in the dissertation, both from a scientific-applied and applied point of view.

2. Degree of knowledge of the state of the problem and creative interpretation of the literary material.

In this doctoral thesis are used 200 literature sources. Most of them are from the last 10 years. This gives me reason to believe that PhD student Eriselda Malaj is familiar with the current state of the problems posed by her, which is the basis for successful solution of the defined tasks.

3. Correspondence of the chosen research methodology with the set goal and tasks of the dissertation.

PhD student Eriselda Malaj has formulated a goal and tasks that are adequate and meet the requirements for dissertation work for obtaining the educational and scientific degree "Doctor".

The literature review identified key challenges and gaps in the field of logical encryption, which are related to: resistance to new attack methodologies, such as those arising from advances in quantum computing; key management challenges and the need for more efficient and scalable encryption mechanisms.

Several weaknesses in hardware security area are indicated, like increased area, delay, and power consumption caused by used logic locking and obfuscation methods. Also there's limited empirical data on how these methods perform under real-world attack scenarios or industrial-scale chip designs. Universal standard for evaluating hardware security is missing. The older techniques, like XOR-based obfuscation, have become less effective to evolving attack methodologies such as machine learning-based reverse engineering and side-channel attacks.

The chosen methodology combines theoretical analysis, hardware design, simulation-based evaluation, and security assessment. The core focus is on developing and evaluating logic-level encryption techniques that enhance circuit security while maintaining acceptable design overhead. The overall includes the following phases: logic encryption design and integration; hardware description and implementation; performance evaluation; security strength assessment; comparative analysis and validation. The logic encryption itself incorporates three distinct data collection methodologies, which are experimental approach, simulation-based approach and valuation and validation approach.

4. Brief analytical description of the doctoral thesis and assessment of the reliability of the material on which the contributions of the dissertation are built.

The presented dissertation consists of 167 pages of text and 153 pages of annexes, very well structured in five chapters, abstract, list of publications, list of cited papers, lists of figures and tables, lists of

abbreviations, introduction, limitations, future work, contributions and references.

In Chapter I is performed literature review. An overview of cybersecurity in communication systems has been provided. Hardware obfuscation method is analyzed. The Register Transfer Level (RTL) obfuscation, Gate-level obfuscation, Layout level obfuscation, Instruction Set obfuscation and PCB obfuscation are described respectively. The hardware design logic encryption process is discussed. Hardware vs. software security approaches are compared. The security problems and vulnerabilities in Integrated Circuit design process are presented. Different types of hardware attacks are listed. The nature and risks connected with hardware trojan attacks, as wells as taxonomy of hardware trojans are explained. Also, different types of attacks such as reverse engineering attacks, side-channel attacks, power analysis attacks, fault injection attacks are described. Different types of cryptographic algorithm implemented in hardware devices are classified and compared. The hardware security challenges and tools and technique in hardware devices security are presented. The most widely used logic encryption techniques XOR/XNOR gates, MUX-based logic, Flip-Flop encryption are reviewed.

The research methods for hardware encryption are presented in Chapter II. A multi-stage methodology to investigate the effective integration, security robustness, and performance trade-offs of logic encryption techniques in digital circuits is adopted. The research follows a design-oriented and experimental approach. The core focus is on developing and evaluating logic-level encryption techniques that enhance circuit security while maintaining acceptable design overhead. The factors Affecting Logic-Encrypted in FPGA designs are analyzed. Different logic encryption architectures are developed to represent both combinational and sequential locking strategies. XOR/XNOR-Based Encryption, MUX-Based Encryption and Flip-Flop-based encryption scheme are described. The hardware implementation flow for logic-encrypted FPGA designs is presented. The effectiveness of logic encryption techniques is evaluated using a combination of hardware performance metrics and security metrics. Key management strategies are analyzed with respect to secure storage, controlled activation, scalable distribution, and key sensitivity. A structured comparative analysis is conducted across all proposed logic

encryption techniques using a unified set of performance and security metrics. The evaluation framework developed in the thesis supports: objective comparison of XOR/XNOR-based, MUX-based, and Flip-Flop-based encryption techniques; identification of optimal trade-offs between hardware overhead (power, area, delay) and security strength; validation of the proposed Flip-Flop-based encryption method.

In Chapter III is presented the implementation and systematic evaluation of hardware logic encryption techniques for enhancing the cybersecurity of communication systems. Three encryption mechanisms: XOR/XNOR-based logic encryption, MUX-based logic encryption, and Flip-Flop-based encryption are investigated. An algorithmic evaluation framework is proposed to quantitatively assess encryption robustness and implementation overhead. The framework integrates logic obfuscation, key-dependent transformations, and state-based encryption to evaluate security strength through fault injection experiments, Hamming distance analysis, and error propagation metrics. The impact of encryption on latency, power consumption, and area overhead is analyzed to characterize performance trade-offs. The proposed encryption techniques are evaluated using standard ISCAS benchmark circuits. The obtained results show that when high or very-high security is required and all metric thresholds are satisfied, the algorithm prioritizes Flip-Flop-based encryption due to its state-dependent behavior, which significantly increases output corruption under incorrect keys, reduces fault observability, and dramatically increases SAT (Boolean Satisfiability) attack complexity.

The experimental test bench for investigating circuits with different types of encryptions gates XOR/XNOR, MUX and Flip-Flop based is created and presented Chapter IV. The research aims to measure the hamming distances for incorrect activation keys between the incorrect and correct output, the corruption factor and the secrecy. The logic circuits are described VHDL language and 3 types of encryption logic techniques are implemented. Three type of logic encryption technique investigated are analyzed: XOR/XNOR-based encryption, MUX-based encryption and flip-flop encryption technique.

In Chapter V are presented simulation and evaluation of hardware solutions for cybersecurity of communication systems. The Average

Hamming Distance (AHD) and Average Fault Sensitivity (AFS) results per ISCAS benchmark circuit are summarized. The obtained results show that Flip-Flop-based encryption consistently achieves the highest AHD and the lowest AFS across all benchmark circuits. The conclusion is that Flip-Flop-based encryption provides superior robustness against functional and fault-based attacks, especially in state-intensive communication hardware. The key observations of the investigations are: AHD increases with circuit size, indicating stronger diffusion in larger designs; AFS decreases for Flip-Flop-based encryption, showing improved fault resilience; sequential circuits benefit most from Flip-Flop-based encryption; XOR/XNOR remains lightweight but offers weaker obfuscation. The analysis of SAT attack runtime per ISCAS Benchmark show that, XOR/XNOR-based encryption is rapidly broken across all benchmarks, whereas MUX-based encryption exhibits moderate resistance. Flip-Flop-based encryption significantly increases SAT solver runtime, particularly for sequential circuits. The performance overhead analysis shows that XOR/XNOR-based encryption incurs the lowest overhead across all benchmarks, while MUX-based encryption introduces moderate increases due to additional selection logic. Flip-Flop-based encryption results in the highest power and delay overhead, particularly in sequential benchmarks. The overall conclusions are: increasing key-gate density consistently improves security metrics; sequential (Flip-Flop-based) encryption provides superior scaling in AHD, AFS, and SAT resistance; XOR/XNOR-based encryption is suitable only for lightweight protection; performance overhead scales predictably and remains manageable for security-critical deployments; the Composite Security Score effectively bridges experimental evaluation and real-world deployment decisions.

5. Scientific, scientific-application and application contribution of the dissertation.

In the doctoral thesis the author has indicated 8 contributions. Four of them are scientific, two of the indicated contributions are scientific-application and two are application contributions. I accept the contributions formulated by the PhD student Eriselda Malaj, which can be summarized as follows:

- A unified framework is developed to quantitatively evaluate logic-encrypted circuits using functional, fault-based, and SAT-based security metrics alongside hardware performance overhead.
- A novel composite metric is proposed to integrate multiple security dimensions into a single score, enabling direct comparison across benchmarks, encryption styles, and key-gate densities.
- Experimental results confirm that Flip-Flop-based, state-dependent encryption provides superior resistance to fault injection and SAT-based attacks compared to purely combinational schemes.
- A threshold-based algorithm is proposed to translate experimental security metrics into deterministic FPGA and ASIC deployment decisions.
- A structured comparison of XOR/XNOR-based, MUX-based, and Flip-Flop-based encryption techniques is presented across both combinational and sequential benchmark circuits.
- The impact of key-gate density on security strength and implementation cost is systematically analyzed for 2, 5, 10, and 16 key-gate configurations.
- Synthesizable VHDL implementations of all encryption techniques are provided, facilitating integration into practical communication-oriented hardware subsystems. The framework is validated on standard ISCAS-85 and ISCAS-89 benchmark circuits, ensuring reproducibility and relevance to real-world digital designs.

I believe that the results obtained are original and fully comply with the requirements for dissertation work for obtaining the educational and scientific degree "Doctor".

6. Assessment of the degree of personal participation of the dissertation in the contributions.

For the personal contributions of the PhD student judges from the fact that she has one independent scientific paper, and in eight of the others she is the first co-author. It is very positive that presented papers of the PhD student have 5 citations. This gives me reason to accept that the dissertation and contributions are the personal work of the candidate.

7. Evaluation of dissertation publications. Reflection in science.

Nine publications and have been made on the dissertation. Three of the papers are reported at conferences in Bulgaria. Eight of the articles are

referenced in Scopus. The PhD student is co-author of a book chapter referenced in Scopus.

The publications made exceed the minimum requirements for the award of the educational and scientific degree "Doctor". I accept that the main results of the dissertation are available to the international and Bulgarian scientific community.

8. Application of the results of the dissertation in scientific and social practice.

It is very positive that the realized researches of the PhD student is developed in the framework of the Joint Doctoral Program in the CEEPUS NETWORK number: CIII-BG-1103-06-2122.

9. Assessment of the compliance of the abstract with the requirements for its preparation, as well as the adequacy of reflecting the main points and contributions of the dissertation.

The abstract fully reflects the content and results obtained in the dissertation, emphasizing the main contributions. Also, the requirements for the preparation of abstracts at the Technical University - Sofia are fully met. Therefore, I gave a positive feedback on its printing.

10. Critical remarks and recommendation

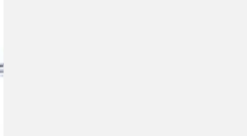
All recommendations and remarks made by me in the preliminary statement, as well as in the preliminary discussion of the dissertation are fulfilled.

11. Conclusion

I believe that the doctoral thesis "Development of new hardware solutions for cybersecurity of communication systems" by PhD student Eriselda Malaj meets the requirements of the Law on the Development of Academic Staff in the Republic of Bulgaria and the Regulations for its implementation. I accept that the conclusions made are logically and competently constructed.

Based on the scientific, scientific-application and applied contributions received in the dissertation, the demonstrated educational level and accumulated theoretical and practical experience, the presented scientific papers, I propose to the Scientific Jury to award the scientific degree "Doctor" in professional field 5.3 Communication and computer engineering, scientific specialty "Computer-aided engineering and computer-aided design systems " to Eriselda Malaj.

24. 08. 2026 r.

Reviewer: 
(Assoc. prof. Tihomir Brusev)