

СТАНОВИЩЕ

върху 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:

маг. Ериселда Малай

Тема на дисертационния труд: „Разработване на нови
хардуерни решения за киберсигурност на
комуникационни системи“

Член на научното жури: доц. д-р инж. Ростислав Русев,
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.

Темата на дисертационния труд е актуална и иновативна, тъй като се фокусира върху методите за логическо криптиране. Чрез тях се осигурява защита и кибер сигурност на интегралните схеми (ИС) срещу обратно инженерство и хардуерна манипулация. В дисертацията са разработени алгоритми и методи за оценка ефективността на криптиране и влиянието му върху консумацията на енергия, заеманата площ и закъснението на схемата.

Целта на дисертацията е да се проектират модули за хардуерно криптиране, използващи логически структури, да се внедрят в комуникационни хардуерни системи, да се оцени и сравни тяхната производителност, използвайки ключови хардуерни показатели (мощност, площ, забавяне), да се оцени силата на сигурност на всеки метод, използвайки показатели като AND, AFS и устойчивост на SAT атаки, и да се предложи нова рамка за оценка на хардуерно криптиране, приложима за комуникационни подсистеми.

Направената справка в научните бази данни показва над 1500 публикации, свързани с Logic encryption, като от 2017 година се забелязва експоненциален ръст на публикациите. Всичко това определя актуалността на изследвания проблем.

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

В тази дисертация са използвани 200 литературни източника. В обзорните глави са цитирани 28 публикации от последните пет години.

Това ми дава основание да смятам, че докторантката Ериселда Малай познава съвременното състояние на решаваните от нея 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“.

За решаване на поставените задачи и постигане на целта на дисертацията са използвани различни методи.

4. Научни, научноприложни и приложни приноси на дисертационния труд

В докторската дисертация могат да се обобщят следните приноси.

Научни приноси:

- Въвеждане на комбинирана оценка за сигурност. Предлага се нова комбинирана метрика за интегриране на множество измерения на сигурността в една оценка, което позволява директно сравнение между бенчмаркове, стилове на криптиране и плътности на ключовите портове.
- Алгоритъм за вземане на решения за внедряване, ориентирани към сигурността и разходите. Предлага се алгоритъм, базиран на праг, за да се преобразуват експериментални показатели за сигурност в детерминистични решения за внедряване на FPGA и ASIC.

Научноприложни приноси:

- Анализ на мащабируемостта на плътността на криптиране. Систематично се анализира влиянието на плътността на ключовите гейтове върху силата на сигурността и разходите за внедряване за конфигурации с 2, 5, 10 и 16 ключови гейта.

Приложни приноси:

- Валидиране, управлявано от бенчмарк, с помощта на ISCAS схеми. Рамката е валидирана върху стандартни бенчмарк схеми ISCAS-85 и ISCAS-89, което гарантира възпроизводимост и релевантност към реални цифрови проекти.
- Готови за внедряване хардуерни модели. Предоставени са синтезируеми VHDL имплементации на всички техники за криптиране, улесняващи интеграцията в практически комуникационно-ориентирани хардуерни подсистеми.

□

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

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

За личните приноси на докторантката Ериселда Малай заключавам от факта, че тя има един самостоятелен научен труд, а в 9 от останалите е съавтор (тя е съавтор и в глава от книга). Това ми дава основание да приема, че дисертационният труд и приносите са лично дело на кандидата.

6. Преценка на публикациите по дисертационния труд.

По дисертацията са направени 9 публикации, като 8 от статиите са реферирани. Докторантката е съавтор в глава от книга, реферирана в Scopus. Представената авторска справка показва 7 цитирания в статии.

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.

7. Критични забележки и препоръки

Нямам сериозни забележки към представената дисертация.

Цитираната литература не е правилно подредена в основния текст.

8. 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 изводите и заключенията в дисертацията са логически и компетентно построени.

Въз основа на получените научноприложни приноси в дисертацията, образователното ниво, натрупания теоретичен и практически опит, значимите публикации по дисертацията, предлагам на научното жури да присъди на маг. 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“.

03.09.2026г.

ЧЛЕН НА ЖУРИТО:

(доц. д-р Ростислав Русев)

04.09.2020

04.09.2020

ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СОФИЯ

STATEMENT

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

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

Author of doctoral thesis:

M.Sc. Eriselda Malaj

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

Assoc. prof. Dr. Eng. Rostislav Rusev,
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.

The topic of the dissertation is relevant and innovative, as it focuses on logic encryption methods. These methods provide protection and cybersecurity for integrated circuits (ICs) against reverse engineering and hardware manipulation. The dissertation develops algorithms and methods for evaluating encryption effectiveness and its impact on power consumption, area overhead, and circuit delay.

The objective of the thesis is to design hardware encryption modules using logic structures, to implement them in communication-related hardware systems, to evaluate and compare their performance using key hardware metrics (power, area, delay), to assess the security strength of each method using metrics such as AHD, AFS, and SAT attack resistance and to propose a new hardware encryption evaluation framework applicable to communication subsystems.

A review of the scientific databases reveals more than 1,500 publications related to Logic encryption, with an exponential growth in publications since 2017. All of this determines the relevance of the researched problem.

2. Degree of understanding of the current state of the problem and creative interpretation of the literature reviewed.

This dissertation uses 200 literary sources. In the review chapters are cited 28 publications from the last five years.

This gives me reason to believe that the PhD student Eriselda Malaj is well acquainted with the current state of the art in the addressed research problems, which is the basis for successfully 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 correspond to the requirements of a dissertation work for acquiring the educational and scientific degree "**Doctor**". Various methods were used to solve the tasks and achieve the goal of the dissertation.

4. Scientific, scientific-applied and applied contribution of the dissertation.

The following contributions can be summarized in the doctoral dissertation.

Scientific contributions:

- **Introduction of a Composite Security Score** 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.

- **Security–Cost Driven Deployment Decision Algorithm** A threshold-based algorithm is proposed to translate experimental security metrics into deterministic FPGA and ASIC deployment decisions.

Scientific-application contribution:

- **Scalability Analysis of Encryption Density** The impact of key-gate density on security strength and implementation cost is systematically analyzed for 2, 5, 10, and 16 key-gate configurations.

Application contributions:

- **Benchmark-Driven Validation Using ISCAS Circuits** The framework is validated on standard ISCAS-85 and ISCAS-89 benchmark circuits, ensuring reproducibility and relevance to real-world digital designs.

- **Implementation-Ready Hardware Models** Synthesizable VHDL implementations of all encryption techniques are provided, facilitating integration into practical communication-oriented hardware subsystems.

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

5. An assessment of the degree of the dissertation candidate's personal participation in the contributions.

For the personal contributions of the PhD student Eriselda Malaj, I judge from the fact that she has one independent scientific paper, and she is co-author in 9 of the others (she is also a co-author in a book chapter). This gives me reason to assume that the dissertation work and contributions are the personal work of the candidate.

6. Evaluation of dissertation publications.

Nine publications have been made on the dissertation, with 8 of the articles being refereed. The PhD student is a co-author of a book chapter referenced in Scopus. The presented author reference shows 7 citations in articles.

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

7. Critical remarks and recommendations.

I have no serious remarks to the presented dissertation.

The cited references are not properly arranged in the main text.

8. Conclusion

I believe that the dissertation "Development of new hardware solutions for cybersecurity of communication systems" by PhD student Eriselda Malaj meets the requirements of the Act on the Development of Academic Staff in the Republic of Bulgaria and its implementing Regulations.

I accept that the conclusions and final remarks in the dissertation are logically and competently constructed.

Based on the scientific and applied contributions received in the dissertation, the educational level, the accumulated theoretical and practical experience, the significant publications on the dissertation, I propose to the scientific jury to award M.Sc. Eriselda Malaj the academic degree "**Doctor**" in professional field 5.3 Communication and Computer Engineering, in the scientific speciality „Computer-aided engineering and computer-aided design systems “.

03.09.2026.

Member of the Scientific Jury:

(Assoc. prof. Rostislav Rusev)