УНИВЕРЗИТЕТ У БЕОГРАДУ - ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ
Булевар краља Александра 73, 11000 Београд, Србија
Тел. 011/324-8464, Факс: 011/324-8681

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена Електротехничког факултета у Београду, на својој седници одржаној 28.05.2019. године, именовало нас је у Комисију за преглед и оцену мастер рада кандидата Николе Кнежевића, дипл. инж. Електротехнике и рачунарства, под насловом „Имплементација и поређење Trivium и Grain алгоритама за шифровање". Након прегледа материјала комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Никола Кнежевић је рођен 24.12.1992. године у Београду. Завршио је основну школу „Десанка Максимовић" у Београду. Уписао је средњу електротехничку школу „Никола Тесла" у Београду и коју је завршио са одличним успехом. Електротехнички факултет уписао је 2011. године. Дипломирао је на одсеку за Телекомуникације и инфромационе технологије 2017. године са просечном оценом 7,13. Дипломски рад одбранио је у септембру 2017. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу системско инжењерство и радио комуникације уписао је у октобру 2017. године. Положио је све испите са просечном оценом 8.

2. Опис мастер рада

Мастер рад обухвата 46 страна, са укупно 28 слика, 7 табела и 8 референци. Рад садржи увод, 4 поглавља, закључак (укупно 6 поглавља), списак коришћене литературе, и списак слика и списак табела.

Предмет рада представља хардверска имплементација два алгоритма за стрим шифровање (Trivium и Grain). Поред тога урађено је и поређење имплементације наведена два алгоритма. Приликом имплементације је коришћен Verilog програмски језик, као и SystemVerilog у оквиру верификације.

У уводном поглављу описан је значај алгоритама за шифровање, као и битне особине које један алгоритам мора да поседује. Потом је дат преглед остатка рада по поглављима.

Друго поглавље је посвећено Trivium алгоритму. У оквиру овог поглавља је описан принцип рада Trivium алгоритма, дата је анализа сигурности на различите типове напада и на крају је изложена реализована хардверска имплементација.

Треће поглавље је конципирано на исти начин као и друго поглавље уз разлику да је треће поглавље посвећено Grain алгоритму.

Четврто поглавље је посвећено тестирању случајности секвенце што је битно код псеудослучајних секвенци које се типично користе у криптографији. Описана су два пакета тестова, при чему су сви тестови описани и објашњена је њихова сврха.

Пето поглавље даје опис поступка верификације. Даје се преглед начина верификације, затим кратак опис UVM, и на крају је описана верификација оба дизајна реализована у оквиру тезе.

Шесто поглавље даје поређење два алгоритма са становишта хардверске имплементације и резимирају се резултати рада. Након тога је дат списак коришћене литературе.

3. Анализа рада са кључним резултатима

Мастер рад Николе Кнежевића, дипл. инж. Електротехнике и рачунарства, је реализовао два алгоритма за шифровање - Trivium и Grain. Основни доприноси рада су следећи:

1) хардверска имплементација Trivium алгоритма;
2) хардверска имплементација Grain алгоритма;
3) обе имплементације су портабилне.

4. Закључак и предлог

Кандидат Никола Кнежевић, дипл. инж. Електротехнике и рачунарства, је у свом мастер раду успешно обрадио тему два алгоритма за стрим шифровање и њихову имплементацију. Никола је показао да познаје област програмирања комуникационог хардвера веома добро. Резултати тезе се могу применити у уређајима који имају потребе за стрим шифровањем. На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад кандидата Николе Кнежевића, дипл. инж. Електротехнике и рачунарства, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 06.09.2019. године

Чланови комисије:

др Зоран Чича, ванр. професор

др Дејан Драјић, ванр. професор