КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 23.4.2024. године именовало нас је у Комисију за преглед и оцену мастер рада дипл. инж. Кристине Живановић под насловом „ Анализа перформанси лаких алгоритама за симетричну енкрипцију у IoT системима". Након прегледа материјала Комисија подноси следећи

И З В Е Ш Т А Ј

1. Биографски подаци кандидата

Кристина Живановић је рођена 19.10.1999. године у Београду. Завршила је основну школу „Сестре Илић" у Ваљеву и Ваљевску гимназију. Војну академију уписала је 2018. године. Дипломирала је на модулу Војноелектронско инжењерство смер Информациони системи 2022. године са просечном оценом 9,96 и била је студент генерације. Дипломски рад „Један приступ имплементацији криптозаштите са краја-на-крај у *IoT* системима„ одбранила је у августу 2022. године са оценом 10. Дипломске академске – мастер студије на Електротехничком факултету у Београду, на Модулу рачунарска техника и информатика уписала је у октобру 2022. године. Положила је све испите са просечном оценом 8,90. Од септембра 2022. године је запослена у Војсци Србије у Центру за примењену математику и електронику.

2. Извештај о студијском истраживачком раду

Кандидат Кристина Живановић је анализирала начин рада криптографског алгоритма Ascon,који спада у класу тзв. лаких криптографских алгоритама, као и особине које чине овај алгоритам погодним за примену у уређајима са ограниченим хардверским ресурсима. Проучене су његове различите имплементације на уређајима који се користе у IoT системима. Затим је дизајниран систем којим је требало да се изврши евалуација рада овог алгоритма у реалним условима и на реалном IoT хардверу. Дизајнирани систем је имплементиран, а анализом перформанси лаког алгоритма Ascon у односу на AES утврђено је да на платформи ESP32 лаки алгоритам постиже 6.7 пута већу брзину енкрипције, док код платформе ArduinoUNO исти алгоритам постиже 2.5 пута већу брзину, чиме су потврђене иницијалне хипотезе о томе да је Ascon алгоритам погодан за примену у IoT апликацијама.

3. Опис мастер рада

Мастер рад обухвата 35 страна, са укупно 17 слика, 2 табеле, 1 графиконом и 25 референци. Рад садржи увод, 4 поглавља и закључак (укупно 6 поглавља), списак коришћене литературе, списак слика и списак скраћеница.

Прво поглавље представља увод у коме су описани предмет и циљ рада. Представљен је значај заштите у IoT системима као и проблеми и ограничења у покушајима заштите истих.

У другом поглављу је описан појам IoT система, безбедносни ризици и сајбер претње и најчешћи напади на овакве система. Такође, представљене су мере превенције у циљу заштите ових система, међу којима је и описан значај лаких алгоритама криптозаштите.

У трећем поглављу се описује породица алгоритама Ascon са акцентном на алгоритме за аутентификовану енкрипцију. Такође, детаљно је описана сама имплементација алгоритма

Ascon128, и најзад су истакнуте предности овог алгоритма у погледу употребе у системима који су ресурсно ограничени. Описане су кључне карактеристике Ascon-а које га сврставају у групу лаких алгоритама.

Четврто поглавље детаљно описује имплементирани прототип IoT система и коришћене технологије. Садржи визуалне приказе хардвера и софтвера који су коришћени и описује протокол за размену информација.

У оквиру петог поглавља представљени су резултати мерења перформанси над прототипом описаним у претходном поглављу. Перформансе су мерене искључиво у контексту времена потребног за извршавање операција енкрипције. Добијени резултати су анализирани, и утврђени су разлози за заначајну разлику у односима времена добијених на две коришћене платформе.

Шесто поглавље је закључак у оквиру кога су резимирани резултати рада, као и његови доприноси. Описан је даљи правац развоја и потенцијалне употребе развијеног система.

4. Анализа рада са кључним резултатима

Мастер рад дипл. инж. Кристина Живановић се бави анализом перформанси лаког криптографског алгортима Ascon на две различите хардверске платформе. Кључни део рада представља опис прототипа IoT система над којим су перформансе и мерене, који је кандидат имплементирала. Основни доприноси рада су: резултати упоредне анализе перформанси два различита алгоритма AES и Ascon на две платформе (ESP32 и ArduinoUNO), као и прототип IoT система, описи коришћених алата, алгоритама и коришћених протокола.

5. Закључак и предлог

Кандидат Кристина Живановић је у свом мастер раду успешно осмислила, конструисала и имплементирала прототип IoT система, као и оценила перформансе представника алгоритама из групе лаке криптографије у односу на AES, као стандард у области заштите информација. Предложено решење може значајно да унапреди методе заштите IoT система, као и да пружи упоредну анализу која може користити при одабиру платформи за ове системе.

Кандидат Кристина Живановић је исказала самосталност и систематичност у своме поступку, као и иновативне елементе у решавању проблематике овог рада.

На основу изложеног, Комисија предлаже Комисији за студије II степена Електротехничког факултета у Београду да рад дипл. инж. Кристина Живановић прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 28.08.2024. године

Чланови комисије:

_____

др Павле Вулетић, в. проф.

_____

Др Жарко Станисављевић, в. проф.