Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 29.5.2020. именовани смо у комисију за одбрану мастер рада под насловом "**Криптографски хеш алгоритам SHA-3**" кандидата **Ане Станковић,** студијски програм Информатика.
Кандидат је 9.9.2020. доставила текст свог рада. Тема рада SHA-3 (Keccak), најновија фамилија стандардних криптографских хеш алгоритама. Алгоритам ради на принципу сунђерасте структуре – упија било коју количину података и избацује тражену количину података, понашајући се као псеудослучајна функција, чији излаз зависи од свих претходних улаза.
Рад је подељен у шест поглавља. Прво поглавље је уводно. У другом поглављу излажу се основни захтеви које треба да задовоље криптографске хеш функције, рођендански напад на хеш алгоритме, као и Меркле-Дамгард и сунђер конструкција хеш функција. У трећем поглављу описује се структура хеш алгоритама из фамилије SHA-3, заснованих на сунђер конструкцији. У четвртом поглављу описују се алтернативне примене овог алгоритма: аутентикациони код поруке, проточна шифра и аутентификовано шифровање. У петом поглављу приказана је једноставна програмска реализација SHA-3, која је верификована упоређивањем са стандардном реализацијом из библиотеке .Net. Приказани су резултати рођенданског напада на верзије са нестандардном дужином излаза од 16, 24, 32, 40 и 48 бита, тј. пронађене су колизије - парови порука ових дужина са истим хеш вредностима;
за поруке дужине 48 бита трајање напада је око 90 минута. Шесто поглавље је закључак, где се указује на неке могуће правце даљег рада у овој области.

Мишљење.

Увидом у текст **Ане Станковић** "Криптографски хеш алгоритам SHA-3" дошли смо до закључка да приложени рад задовољава у потпуности захтеве који се постављају при изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 23.9.2020.

Др Миодраг Живковић, ред. проф., ментор

Др Александар Картељ, доцент

Др Стефан МИшковић, доцент