УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ – 4**
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ИЗВЕШТАЈ О ОЦЕНИ ПОДОБНОСТИ ТЕМЕ, КАНДИДАТА И МЕНТОРА ЗА ИЗРАДУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

I ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију: Наставно-научно веће Факултета техничких наука

Датум именовања комисије: 26.3.2026.

Састав комисије именоване у складу са *Правилима докторских студија Универзитета у Новом Саду*:

1.	др Огњановић Зоран	Научни саветник	Математичке науке
	презиме и име	звање	ужа научна област
	Математички институт САНУ	председник	
	установа у којој је запослен-а	функција у комисији	
2.	др Гилезан Силвиа	Редовни професор	Теоријска и примењена математика
	презиме и име	звање	ужа научна област
	Универзитет у Новом Саду, Факултет техничких наука	члан	
	установа у којој је запослен-а	функција у комисији	
3.	др Марић Филип	Редовни професор	Рачунарство и информатика
	презиме и име	звање	ужа научна област
	Универзитет у Београду, Математички факултет	члан	
	установа у којој је запослен-а	функција у комисији	
4.	др Урошевић Драган	Редовни професор	Рачунарске науке
	презиме и име	звање	ужа научна област
	Универзитет “Унион”, Рачунарски факултет	члан	
	установа у којој је запослен-а	функција у комисији	
5.	др Сладић Горан	Редовни професор	Примењене рачунарске науке и информатика
	презиме и име	звање	ужа научна област
	Универзитет у Новом Саду, Факултет техничких наука	члан	
	установа у којој је запослен-а	функција у комисији	
6.	др Милосављевић Бранко	Редовни професор	Примењене рачунарске науке и информатика
	презиме и име	звање	ужа научна област
	Универзитет у Новом Саду, Факултет техничких наука	члан	
	установа у којој је запослен-а	функција у комисији	

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: Синиша, Станиша, Томовић
2. Датум рођења: 22.5.1986. Место и држава рођења: Београд, Србија

II.1 Основне или интегрисане студије

Година уписа: 2005 Година завршетка: 2011 Просечна оцена током студија: 9,91

Универзитет: Универзитет у Београду

Факултет: Математички факултет

Студијски програм: Професор математике и рачунарства

Стечено звање: Дипломирани математичар

II.2 Мастер или магистарске студије

Година уписа: 2011 Година завршетка: 2013 Просечна оцена током студија: 10,00

Универзитет: Универзитет у Београду

Факултет: Математички факултет

Студијски програм: Математика

Стечено звање: Мастер математичар

Научна област: Математика

Наслов завршног рада: Кружни снопови и трансформације у еуклидском моделу инверзивног простора

II.3 Докторске студије

Година уписа: 2013

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Математика у техници

Број ЕСПБ до сада остварених: 120 Просечна оцена током студија: 10,00

II.4 Приказ научних и стручних радова кандидата

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
1.	Tomović, S., Knežević, M., Mihaljević, M. J., "Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols", *Mathematics*, vol. 9(5) (2021), 573, DOI: 10.3390/math9050573.	M21a+
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
2.	Knežević, M., Tomović, S., Mihaljević, M. J., "Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation", *Electronics*, vol. 9(8) (2020), 1296, DOI: 10.3390/electronics9081296.	M22
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
3.	Tomović, S., Mihaljević, M. J., Perović, A., Ognjanović, Z., "A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One", *Mathematical Problems in Engineering*, vol. 2016, Article ID 9289050, pp. 1–9, DOI: 10.1155/2016/9289050	M22
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
4.	Tomović, S., Knežević, M., Mihaljević, M. J., Perović, A., Ognjanović, Z., "Security evaluation of NHB# authentication protocol against a MIM attack", *IPSI BgD Transactions on Internet Research (TIR)*, vol. 12(2) (2016), pp. 22-36, ISSN: 1820-4511.	M53
Рад припада проблематици докторске дисертације:	**ДА** НЕ ДЕЛИМИЧНО	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија
5.	Knežević, M., Tomović, S., Mihaljević, M. J., "Attack Scenarios and Security Analysis of a Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks", *IEEE Internet of Things Journal*, vol. 12(23) (2025), pp. 51010–51025, DOI: 10.1109/JIOT.2025.3612005	M21a+
Рад припада проблематици докторске дисертације:	ДА НЕ **ДЕЛИМИЧНО**	

Р. бр.	аутори, наслов рада, *часопис*, **волумен** (година) странице од-до, DOI или ISBN/ISSN	категорија

6.	Tomović, S., Ognjanović, Z., Doder, D., "A First-order Logic for Reasoning about Knowledge and Probability", *ACM Transactions on Computational Logic*, vol. 21(2) (2020), pp. 16:1–16:30, DOI: 10.1145/3359752	M22

Рад припада проблематици докторске дисертације: ДА **НЕ** ДЕЛИМИЧНО

III ОЦЕНА ПОДОБНОСТИ ТЕМЕ

Оцена:

III.1 формулације наслова тезе

Дизајн и напади на класу RFID аутентификационих протокола чија је сигурност заснована на тешком LPN проблему

Design and attacks on a class of RFID authentication protocols whose security is based on the hard LPN problem

Комисија сматра да је предложени наслов тезе подобан.

Предложени наслов тезе је подобан? ДА

III.2 предмета (проблема) истраживања

RFID технологија (Radio Frequency Identification) подразумева употребу радио-таласа за идентификацију и праћење објеката, људи и животиња. Ова технологија спада међу глобално најзаступљеније, са најистакнутијим применама у ланцима снабдевања, као и безбедносним, здравственим, индустријским и транспортним системима.

Основу класичног RFID система чине три компоненте: таг, читач и back-end сервер. Таг је мали електронски уређај ограничених рачунарских ресурса, који похрањује идентификационе податке објекта коме је придружен. Читач комуницира са тагом путем радио-таласа ради очитавања идентитета објекта, и потом прикупљене податке прослеђује серверу ради њихове даље обраде.

Да би се онемогућило лажно представљање тага у RFID систему, након поступка идентификације извршава се и аутентификација — доказивање изјављеног идентитета. Унапред договорена правила по којима се аутентификација одвија чине аутентификациони протокол. RFID аутентификациони протоколи најчешће се ослањају на механизам изазова и одговора, у коме читач шаље упите (изазове) тагу и анализира његове одговоре како би утврдио да ли таг познаје, тј. чува заједничку тајну вредност (кључ). Међутим, тајни кључеви ових протокола су мета најразноврснијих напада, попут прислушкивања комуникације тага и читача, и покушаја реконструкције тајног кључа криптоанализом размењених порука. Један од метода одбране од оваквих напада је примена тзв. редукције на тежак математички проблем, где је нападач принуђен да га реши ако жели сазнати тајни кључ на основу порука, при чему се за тај проблем претпоставља да није решив у полиномијалном времену са незанемарљивом вероватноћом.

Главни предмет истраживања ове дисертације је група RFID аутентификационих протокола чија је сигурност[1], у одговарајућим моделима напада, доказана редукцијом на тзв. тешки LPN проблем (Learning Parity with Noise). LPN проблем подразумева реконструкцију решења зашумљеног система линеарних једначина над бинарним пољем, где је свакој једначини потенцијално додат бит грешке са одређеном вероватноћом. Та група протокола позната је под називом HB фамилија, по свом првом представнику — HB протоколу. До данас је објављено неколико десетина протокола из ове фамилије, и њена еволуција представља низ унапређења усмерених ка повећању безбедности уз што мању потрошњу рачунарских ресурса. Карактеристични напади на HB фамилију укључују: прислушкивање порука између тага и читача (пасивни напад), лажно представљање као читач (активни напад), као и MIM напад (man-in-the-middle), који подразумева да је нападач способан и да прислушкује, као и да модификује све размењене поруке, и да прати одлуке читача о прихватању тага.

Истраживање у оквиру дисертације усмерено је на дизајн нових штедљивих и безбедних протокола из ове фамилије, као и на развој и оптимизацију напада на постојеће протоколе, чиме се непосредно доприноси унапређењу безбедности RFID система.

Комисија констатује да је предмет истраживања подобан за израду докторске дисертације, имајући у виду актуелност и научну утемељеност теме, као и њен потенцијал да резултира

[1] У овом извештају термини „сигурност” и „безбедност” се користе као уобичајени, синонимни преводи енглеског термина "security".

иновативним научним доприносима и да подстакне даља истраживања у овој области.

Предмет истраживања је подобан? **ДА**

III.3 познавања проблематике на основу изабране литературе са списком литературе

Преглед релевантне литературе указује на то да RFID аутентификациони протоколи представљају добро развијену и веома активну област истраживања. Општи и систематски прегледи RFID технологије [1], [2] бележе њене бројне примене у ланцима снабдевања, безбедносним системима, IoT окружењима, логистици, транспорту и здравству. Прегледни радови о RFID аутентификацији [3]–[5] истичу да ограничени рачунарски и енергетски ресурси тагова намећу потребу за штедљивим (lightweight) протоколима и условљавају њихову класификацију према сложености подржаних операција. У том смислу, литература доследно издваја HB фамилију као једну од значајних класа штедљивих аутентификационих протокола у RFID окружењу [6], [7].

Полазну основу ове истраживачке линије представља HB протокол [8], предложен за аутентификацију људи преко несигурног канала, чија је сигурност од пасивних напада доказана редукцијом на LPN проблем. Рад [9] проширује ту идеју увођењем HB+ протокола, прилагођеног аутентификацији уређаја, уз додатни тајни вектор и маскирајућу поруку тага који обезбеђују отпорност на активне нападе. Међутим, убрзо је у [10] демонстриран успешан GRS man-in-the-middle напад на HB+, у ком нападач мења поруке читача и на основу исхода аутентификације постепено издваја информације о тајном кључу. Након тога су предложена бројна унапређења HB+ протокола усмерена ка јачању отпорности на GRS-MIM тип напада, као што су HB++ [11], HB* [12], HB-MP' и HB-MP [6] – но испоставило се да су му и они подложни [13].

Први протокол за који је формално доказана сигурност од GRS-MIM напада био је Random-HB# [14]. У њему се, уместо тајних вектора које користи HB+, уводе две тајне матрице ради достизања зацртаног нивоа безбедности, што повлачи и веће меморијско заузеће. Ради ублажавања тог недостатка, у истом раду предложен је и HB#, који задржава исту основну структуру, али користи Теплицове матрице као штедљивије тајне кључеве. Додатно унапређење представља NHB# [15], код кога се чува само једна тајна матрица, док је друга замењена посебно конструисаном случајно изабраном циркуларном матрицом, чиме се меморијски захтеви смањују уз очување истог нивоа сигурности. Поред Random-HB# и NHB# у литератури су предложени и други наследници HB+ протокола који уводе различите механизме отпорности на MIM напад, о чему извештавају радови [7], [16].

Паралелно са развојем одбрамбених механизама развијале су се и криптоаналитичке технике. Тако је у [17] представљен општи MIM напад на Random-HB# и HB#, познат као OOV-MIM, при чему су аутори тврдили да се исти приступ може применити и на све до тада познате протоколе HB фамилије. Тај напад је у [18] искоришћен као black-box компонента у нападу на NHB# протокол. Међутим, накнадна емпиријска анализа у [19] утврдила је да OOV-MIM није био толико ефикасан као што је првобитно наведено, па је у [20] предложен његов редизајн, уз прецизнију анализу и експерименталну потврду побољшаних перформанси. Ови резултати потврђују да се развој HB фамилије у литератури одвија кроз сталну интеракцију дизајна протокола и њихове криптоанализе.

Шири преглед литературе открива да HB фамилија припада већој групи штедљивих аутентификационих решења заснованих на различитим варијантама LPN проблема и сродним тешким задацима. У том оквиру посебно се издвајају Lapin [21], који се ослања на Ring-LPN, AUTH [22], заснован на Subspace-LPN проблему, као и RSDP HB+ протокол [23], који користи Restricted Syndrome Decoding Problem. Посебно место има и LCMQ протокол [24], предложен као хибридно штедљиво решење које комбинује LPN проблем са тешким мултиваријантним квадратним проблемом, али је касније показано да је рањив и на хардверског „тројанског коња“

[25] и на реконструкцију тајног кључа [26].

У литератури се истиче и група атипичних, нелинеарних представника HB фамилије, као што су GHB# [27], NLHB [28] и HBN [29], код којих је напуштено уобичајено линеарно својство одговора тага. Ови радови сведоче о томе да се развој HB фамилије није одвијао само кроз појачавање отпорности на познате нападе, већ и кроз тражење нових дизајнерских приступа у оквиру исте основне идеје.

Поред теоријских доприноса, у литератури се протоколи HB фамилије и сродна LPN-заснована решења за аутентификацију интегришу као безбедносна компонента практичних система у различитим областима. Наводе се примене у саобраћају [30], [31], IoT окружењима [32], [33], индустријским системима, укључујући Modbus TCP мреже [34], као и у fog рачунарству и паметној енергетици [35].

На основу прегледа литературе може се закључити да HB фамилија протокола представља област са добро развијеном теоријском основом, богатом праксом дизајна и криптоанализе, и јасно уочљивим отвореним питањима.

Списак литературе

[1] Munoz-Ausecha, C., Ruiz-Rosero, J., Ramirez-Gonzalez, G., "RFID Applications and Security Review", *Computation*, vol. 9(6), 69, 2021, doi:10.3390/computation9060069.
[2] Haibi, A., Oufaska, K., El Yassini, K., Boulmalf, M., Bouya, M., "Systematic Mapping Study on RFID Technology", *IEEE Access*, vol. 10, pp. 6363-6380, 2022, doi:10.1109/ACCESS.2022.3140475.
[3] Ibrahim, A., Dalkilic, G., "Review of different classes of RFID authentication protocols", *Wireless Networks*, vol. 25(3), pp. 961-974, 2019, doi:10.1007/s11276-017-1638-3.
[4] Mohsin, S. M., Khan, I. A., Akber, S. M. A., Shamshirband, S., Chronopoulos, A. T., "Exploring the RFID mutual authentication domain", *International Journal of Computers and Applications*, vol. 43(2), pp. 127-141, 2021, doi:10.1080/1206212X.2018.1533614.
[5] Kumar, A., Jain, A. K., Dua, M., "A comprehensive taxonomy of security and privacy issues in RFID", *Complex & Intelligent Systems*, vol. 7(3), pp. 1327-1347, 2021, doi:10.1007/s40747-021-00280-6.
[6] Munilla, J., Peinado, A., "HB-MP: A further step in the HB-family of lightweight authentication protocols", *Computer Networks*, vol. 51(9), pp. 2262-2267, 2007, doi:10.1016/j.comnet.2007.01.011.
[7] Aseeri, A., Bamasag, O., "Achieving protection against man-in-the-middle attack in HB family protocols implemented in RFID tags", *International Journal of Pervasive Computing and Communications*, vol. 12(3), pp. 375-390, 2016, doi:10.1108/IJPCC-03-2016-0015.
[8] Hopper, N. J., Blum, M., "Secure Human Identification Protocols", *ASIACRYPT 2001*, vol. LNCS 2248, pp. 52-66, 2001, doi:10.1007/3-540-45682-1_4.
[9] Juels, A., Weis, S. A., "Authenticating Pervasive Devices with Human Protocols", *CRYPTO 2005*, vol. LNCS 3621, pp. 293-308, 2005, doi:10.1007/11535218_18.
[10] Gilbert, H., Robshaw, M. J. B., Sibert, H., "Active attack against HB+: a provably secure lightweight authentication protocol", *Electronics Letters*, vol. 41(21), pp. 1169-1170, 2005, doi:10.1049/el:20052622.
[11] Bringer, J., Chabanne, H., Dottax, E., "HB++: a Lightweight Authentication Protocol Secure against Some Attacks", *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006)*, IEEE, pp. 28-33, 2006, doi:10.1109/SECPERU.2006.10.
[12] Duc, D. N., Kim, K., "Securing HB+ against GRS Man-in-the-Middle Attack", *Proceedings of the 2007 Symposium on Cryptography and Information Security (SCIS 2007)*, pp. 23-26, 2007.
[13] Gilbert, H., Robshaw, M. J. B., Seurin, Y., "Good Variants of HB+ Are Hard to Find", *Financial Cryptography and Data Security, FC 2008*, vol. LNCS 5143, pp. 156-170, 2008, doi:10.1007/978-3-540-85230-8_12.
[14] Gilbert, H., Robshaw, M. J. B., Seurin, Y., "HB#: Increasing the Security and Efficiency of HB+", *EUROCRYPT 2008*, vol. LNCS 4965, pp. 361-378, 2008, doi:10.1007/978-3-540-78967-3_21.
[15] Tomović, S., Mihaljević, M. J., Perović, A., Ognjanović, Z., "A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One", *Mathematical Problems in Engineering*, vol. 2016, Article ID 9289050, pp. 1-9, doi:10.1155/2016/9289050.
[16] Hamann, M., "Lightweight Cryptography on Ultra-Constrained RFID Devices", PhD thesis, University of Mannheim, 2018.

[17] Ouafi, K., Overbeck, R., Vaudenay, S., "On the Security of HB# against a Man-in-the-Middle Attack", *ASIACRYPT 2008*, vol. LNCS 5350, pp. 108-124, 2008, doi:10.1007/978-3-540-89255-7_8.
[18] Tomović, S., Knežević, M., Mihaljević, M. J., Perović, A., Ognjanović, Z., "Security evaluation of NHB# authentication protocol against a MIM attack", *IPSI BgD Transactions on Internet Research (TIR)*, vol. 12(2), pp. 22-36, 2016, ISSN: 1820-4511.
[19] Knežević, M., Tomović, S., Mihaljević, M. J., "Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation", *Electronics*, vol. 9(8), 1296, 2020, doi:10.3390/electronics9081296.
[20] Tomović, S., Knežević, M., Mihaljević, M. J., "Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols", *Mathematics*, vol. 9(5), 573, 2021, doi:10.3390/math9050573.
[21] Heyse, S., Kiltz, E., Lyubashevsky, V., Paar, C., Pietrzak, K., "Lapin: An Efficient Authentication Protocol Based on Ring-LPN", *FSE 2012*, vol. LNCS 7549, pp. 346-365, 2012, doi:10.1007/978-3-642-34047-5_20.
[22] Kiltz, E., Pietrzak, K. Z., Venturi, D., Cash, D., Jain, A., "Efficient authentication from hard learning problems", *Journal of Cryptology*, vol. 30(4), pp. 1238-1275, 2017, doi:10.1007/s00145-016-9247-3.
[23] Johansson, T., Khairallah, M., Nguyen, V., "Efficient Authentication Protocols from the Restricted Syndrome Decoding Problem", *Proceedings - IEEE 10th European Symposium on Security and Privacy, Euro S&P 2025*, pp. 845-860, 2025, doi:10.1109/EuroSP63326.2025.00053.
[24] Li, Z., Gong, G., Qin, Z., "Secure and Efficient LCMQ Entity Authentication Protocol", *IEEE Transactions on Information Theory*, vol. 59(6), pp. 4042-4054, 2013, doi:10.1109/TIT.2013.2253892.
[25] Bagadia, K., Chatterjee, U., Basu Roy, D., Mukhopadhyay, D., Chakraborty, R. S., "Exploiting Safe Error based Leakage of RFID Authentication Protocol using Hardware Trojan Horse", *IACR Cryptology ePrint Archive*, Report 2016/1149, 2016.
[26] Nguyen, V., Johansson, T., Guo, Q., "A Key-Recovery Attack on the LCMQ Authentication Protocol", *ISIT 2024*, pp. 1824-1829, 2024, doi:10.1109/ISIT57864.2024.10619211.
[27] Rizomiliotis, P., Gritzalis, S., "GHB#: A Provably Secure HB-Like Lightweight Authentication Protocol", *ACNS 2012*, vol. LNCS 7341, pp. 489-506, 2012, doi:10.1007/978-3-642-31284-7_29.
[28] Madhavan, M., Thangaraj, A., Viswanathan, K., Sankarasubramaniam, Y., "NLHB: A Light-Weight, Provably-Secure Variant of the HB Protocol Using Simple Non-Linear Functions", *NCC 2010*, pp. 1-5, 2010, doi:10.1109/NCC.2010.5430152.
[29] Bosley, C., Haralambiev, K., Nicolosi, A., "HBN: An HB-like protocol secure against man-in-the-middle attacks", *IACR Cryptology ePrint Archive*, Report 2011/350, 2011.
[30] Jadoon, A. K., Wang, L., Zia, M. A., "HB-protocol Based Advance Security System for PKES Using Multiple Antennas", *China Communications*, vol. 15(12), pp. 98-110, 2018, doi:10.12676/j.cc.2018.12.008.
[31] Jadoon, A. K., Li, J., Wang, L., "Physical layer authentication for automotive cyber physical systems based on modified HB protocol", *Frontiers of Computer Science*, vol. 15(3), 153809, 2021, doi:10.1007/s11704-020-0010-4.
[32] Arafin, M. T., Shen, H., Tehranipoor, M. M., Qu, G., "LPN-based Device Authentication Using Resistive Memory", *Proceedings of the 2019 Great Lakes Symposium on VLSI*, pp. 9-14, 2019, doi:10.1145/3299874.3317970.
[33] Mamun, M., Miyaji, A., Luv, R., Su, C., "A lightweight multi-party authentication in insecure reader-server channel in RFID-based IoT", *Peer-to-Peer Networking and Applications*, vol. 14(2), pp. 708-721, 2021, doi:10.1007/s12083-020-01007-z.
[34] Fagundes, F. D., da Cunha, M. J., "Industrial Network Security: HB-MP* as an Authentication Technique for Modbus TCP", *Journal of Control, Automation and Electrical Systems*, vol. 33(4), pp. 1177-1187, 2022, doi:10.1007/s40313-021-00889-5.
[35] Lu, S., Li, X., "Quantum-Resistant Lightweight Authentication and Key Agreement Protocol for Fog-Based Microgrids", *IEEE Access*, vol. 9, pp. 27588-27600, 2021, doi:10.1109/ACCESS.2021.3058180.

На основу пописа литературе који је наведен приликом пријаве теме докторске дисертације, Комисија констатује да је кандидат детаљно проучио релевантну и актуелну научну грађу. Приложене библиографске јединице представљају адекватну основу за реализацију истраживања.

Избор литературе је одговарајући? **ДА**

III.4 циљева истраживања

Циљеви истраживања:

1) Дизајн нових LPN-заснованих аутентификационих протокола који су напреднији у односу на претходне предлоге из ове класе. Унапређење се очекује у погледу отпорности на различите релевантне моделе напада из литературе и/или у погледу штедљивости — сложености рачунских операција, заузећа меморије или обима комуникације тага и читача при аутентификацији.

2) Развој нових напада на LPN-засноване протоколе. Овај циљ обухвата преглед објављених протокола и анализу њихове рањивости на карактеристичне моделе напада HB фамилије. Такође, испитаће се ваљаност постојећих доказа безбедности, будући да они нису увек коректно изведени, чиме се отвара простор за конструкцију нових напада.

3) Евалуација, корекција и оптимизација постојећих напада на LPN-засноване протоколе. Одређени напади у литератури предложени су искључиво у описном или теоријском облику, те је потребно спровести емпиријску анализу, и по потреби кориговати нападе чија изјављена ефикасност заостаје за експерименталном. Поред тога, истражиће се могућности оптимизације алгоритама постојећих напада ради повећања њихове ефикасности.

Комисија закључује да су наведени циљеви истраживања адекватно постављени и подобни за израду докторске дисертације.

Циљеви истраживања су одговарајући? **ДА**

III.5 очекиваних резултата (хипотезе)

Очекује се да резултат истраживања буде дизајн нових LPN-заснованих аутентификационих протокола који ће бити напреднији у односу на постојеће представнике HB фамилије, било у погледу вишег нивоа безбедносне отпорности на релевантне моделе напада, било у погледу мање потрошње рачунарских ресурса, или комбинацијом оба аспекта. Поред тога, предвиђен је развој нових ефикасних напада на одабране протоколе из ове класе, што ће омогућити боље разумевање њихових безбедносних ограничења. Такође се очекује евалуација и, по потреби, корекција постојећих напада, укључујући емпиријску анализу њихове ефикасности и потенцијалну оптимизацију алгоритама.

Комисија сматра да су наведени очекивани резултати добро дефинисани, да представљају значајан истраживачки допринос и да чине основу за реализацију даљих истраживања и примену у предметној области.

Очекивани резултати представљају значајан научни допринос? **ДА**

III.6 плана рада (на основу фаза истраживања и оријентационог садржаја дисертације из Обрасца 1)

Фазе истраживања:

- Утврђивање и спецификација проблема
- Сагледавање актуелног стања у области кроз опсежан преглед литературе
- Конструкција новог LPN-заснованог аутентификационог протокола
- Криптоанализа одабраних LPN-заснованих протокола и проналажење ефикасних напада
- Евалуација објављених напада уз пратећу експерименталну анализу, и њихова корекција или оптимизација
- Дискусија резултата и извођење закључака

Оријентациони садржај докторске дисертације:

1. *Увод (RFID технологија)* — Ово поглавље пружа општи увод у RFID технологију, њене основне компоненте и подручја примене, уз мотивацију истраживања.

2. *RFID аутентификациони протоколи* — Ово поглавље садржи уводне концепте аутентификације у RFID системима, укључујући формалне моделе напада и преглед општих приступа.
3. *HB фамилија RFID аутентификационих протокола* — У овом поглављу се даје детаљан преглед и класификација протокола из HB фамилије.
4. *Преглед литературе о HB фамилији* — Ово поглавље систематизује актуелне радове и трендове у области HB фамилије и LPN-заснованих протокола.
5. *Дизајн новог протокола HB фамилије* — У овом поглављу разматра се дизајн новог LPN-заснованог аутентификационог протокола из HB фамилије.
6. *Напад на објављен протокол HB фамилије* — Ово поглавље представља нов напад на одабрани објављени протокол из HB фамилије.
7. *Унапређење напада на протоколе HB фамилије* — Ово поглавље обухвата евалуацију, корекцију и оптимизацију постојећих напада.
8. *Закључак и будући рад* — Ово поглавље сумира добијене резултате и указује на правце даљих истраживања.
9. *Литература*.

Комисија сматра да је план рада адекватно дефинисан и у складу са очекиваним резултатима истраживања.

План рада је одговарајући? **ДА**

III.7 метода и узорака истраживања

Методолошки оквир доказивања безбедности протокола подразумева формалну спецификацију модела напада (пасивни, активни, GRS-MIM или MIM) на протокол. Безбедност се потом доказује техником редукције на тешки LPN проблем, при чему се сваки успешан нападач алгоритамски трансформише у ефикасан решавач неке варијанте тог проблема. Ова трансформација омогућава квантификацију вероватноће разбијања протокола у односу на вероватноћу решавања посматране инстанце LPN проблема.

Анализа потрошње ресурса предложеног протокола укључује пребројавање елементарних операција које он извршава, разматрање димензија тајних вредности у меморији и обима порука које размењују таг и читач. На основу тих вредности извршиће се поређење штедљивости протокола у односу на претходне чланове HB фамилије.

Експериментална ефикасност посматраног напада испитиваће се нумеричком симулацијом у MATLAB-у, при чему ће бити утврђена емпиријска вероватноћа реконструкције тајног кључа при задатим параметрима протокола и рачунарским ресурсима напада. Величина узорка зависиће од параметарске структуре анализираних протокола.

Комисија сматра да предложене методе одговарају потребама истраживања.

Метод и узорак су одговарајући? **ДА**

III.8 места, лабораторије и опреме за истраживачки рад

Рачунарски ресурси Математичког института САНУ

Услови за истраживачки рад су одговарајући? **ДА**

III.9 методе статистичке обраде података и осталих релевантних података

Није предвиђена статистичка обрада података.

Предложене методе су одговарајуће? **ДА**

IV ОЦЕНА ПОДОБНОСТИ КАНДИДАТА

Услови дефинисани за кандидата студијским програмом:

На основу Закона о високом образовању, као и у складу са Правилима докторских студија Универзитета у Новом Саду, која су усвојена на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, и која су ступила на снагу 5.3.2021., а примењују се од 1.4.2021. године (Измене и допуне: 27.10.2022. године; 30.3.2023. године; 28.3.2024. године и 30.9.2025. године) и према Правилнику о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности Факултета техничких наука (број 01-195/11-1) од 7.10.2021. године, право да пријави тему докторске дисертације стиче студент докторских студија који је положио све испите одређене студијским програмом и који је одбранио Теоријске основе докторске дисертације.

Образложење:

Кандидат Синиша Томовић положио је све испите одређене студијским програмом Математика у техници и одбранио Теоријске основе докторске дисертације, чиме је стекао укупно 120 ЕСПБ. Преосталих 60 ЕСПБ стиче се спровођењем истраживања, као и израдом и одбраном докторске дисертације. Кандидат је такође аутор, односно коаутор, два рада категорије М21а+, три рада категорије М22 и једног рада категорије М53, при чему су четири рада непосредно посвећена тематици предложене дисертације. То показује да се кандидат на адекватан начин и у довољној мери ангажовао као истраживач.

Комисија закључује да кандидат испуњава формалне услове и поседује научну и стручну компетентност за израду докторске дисертације.

Да ли кандидат испуњава дефинисане услове? **ДА**

V ОЦЕНА ПОДОБНОСТИ ПРЕДЛОЖЕНОГ МЕНТОРА

V.1 Биографија ментора (до 500 речи):

Др Миодраг Ј. Михаљевић је дописни члан Српске академије наука и уметности, научни саветник и заменик директора Математичког института САНУ, као и руководилац Националног центра за сајбер безбедност и приватност. Наставник је на докторским студијама студијског програма Математика у техници Факултета техничких наука у Новом Саду.

Дипломирао је 1979. године на Електротехничком факултету Универзитета у Београду, где је и магистрирао 1981. године, а докторску дисертацију одбранио је 1990. године на Војнотехничкој академији ЈНА у Загребу. Своју професионалну каријеру започео је 1979. године у Институту за примењену математику и електронику, где је радио до 1998. године. Од 1992. до 1998. године био је спољни сарадник Математичког института САНУ, а од 1998. године стално је запослен у овој институцији, где је 1999. године изабран за научног саветника, а од 2015. године обавља функцију заменика директора.

Аутор је преко 75 радова објављених у водећим међународним научним часописима као што су IEEE Transactions on Information Theory, IEEE Transactions on Communications, IEEE Communications Letters и други. Учествовао је на више од 50 међународних конференција, објавио преко 50 радова у националним публикацијама, као и више од 50 патената, софтвера и техничких извештаја. Његови радови су цитирани више од 3000 пута.

Био је руководилац бројних националних и међународних пројеката у областима криптологије, обраде слика и рачунарске топологије. Тренутно је ангажован као Distinguished Professor у Shandong Computer Science Center, Qilu University of Technology (Shandong Academy of Sciences), у Ђинану, Кина, а претходно је имао гостујуће позиције у Јапану, укључујући Универзитет у Токију, SONY Computer Science Laboratories и AIST. За свој научни рад добио је више признања, укључујући Награду САНУ за десетогодишња остварења (2003–2012); 2014. године изабран је за

члана Academia Europaea, а 2021. године за дописног члана САНУ. Налази се на „Станфордској листи“ 2% најбољих светских научника за период 2020–2025.

Поред научног рада, др Михаљевић је активан као помоћни уредник и члан уредничких одбора више међународних часописа, и више пута је био члан Матичног одбора ресорног министарства у Србији.

V.2 Референце ментора из научне области којој припада тема докторске дисертације:

Р. бр.	аутори, наслов, *часопис*, **волумен** (година) број страница од-до, DOI или ISBN/ISSN	категорија
1	Tomović, S., Knežević, M., **Mihaljević, M. J.**, "Analysis and Correction of the Attack against the LPN-Problem Based Authentication Protocols", *Mathematics*, vol. 9(5) (2021), 573, DOI: 10.3390/math9050573.	M21a+
2	Knežević, M., Tomović, S., **Mihaljević, M. J.**, "Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation", *Electronics*, vol. 9(8) (2020), 1296, DOI: 10.3390/electronics9081296.	M22
3	Tomović, S., **Mihaljević, M. J.**, Perović, A., Ognjanović, Z., "A Protocol for Provably Secure Authentication of a Tiny Entity to a High Performance Computing One", *Mathematical Problems in Engineering*, vol. 2016, Article ID 9289050, pp. 1–9, DOI: 10.1155/2016/9289050	M22
4	**Mihaljević, M. J.**, Tomović, S., Knežević, M., "An Improved Man-in-the-Middle Attack Against HB# Authentication Protocols", *COST Cryptanalysis of Ubiquitous Computing Systems (CRYPTACUS) Workshop*, 2017, pp. 163-202.	M30
5	Tomović, S., Knežević, M., **Mihaljević, M. J.**, Perović, A., Ognjanović, Z., "Security evaluation of NHB# authentication protocol against a MIM attack", *IPSI BgD Transactions on Internet Research (TIR)*, vol. 12(2) (2016), pp. 22-36, ISSN: 1820-4511.	M53
6	Fossorier, M. P. C., **Mihaljević, M. J.**, Imai, H., Cui, Y., Matsuura, K., "An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication", *INDOCRYPT 2006*, Lecture Notes in Computer Science, vol. 4329 (2006), pp. 48-62, DOI: 10.1007/11941378_5.	M23
7	**Mihaljević, M. J.**, Watanabe, H., Imai, H., "A Cellular Automata Based HB#-like Low Complexity Authentication Technique", *Proceedings of the 2008 International Symposium on Information Theory and Its Applications (ISITA 2008)*, 2008, pp. 1355-1360.	M30
8	Knežević, M., Tomović, S., **Mihaljević, M. J.**, "Attack Scenarios and Security Analysis of a Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks", *IEEE Internet of Things Journal*, vol. 12(23) (2025), pp. 51010–51025, DOI: 10.1109/JIOT.2025.3612005	M21a+
9	**Mihaljević, M. J.**, "A Security Enhanced Encryption Scheme and Evaluation of Its Cryptographic Security", *Entropy*, vol. 21(7) (2019), 701, DOI: 10.3390/e21070701	M21
10	**Mihaljević, M. J.**, Radonjić, A., Wang, L., Xu, S., "Security Enhanced Symmetric Key Encryption Employing an Integer Code for the Erasure Channel", *Symmetry*, vol. 14(8) (2022), 1709, DOI: 10.3390/sym14081709	M21
11	**Mihaljević, M. J.**, Radonjić, A., Mijajlović, N., Wang, L., Xu, S., "An Integer Erasure Correction Coding and Its Application for Security Enhancement of Encryption", *IEEE Access*, vol. 13 (2025), pp. 104728–104741, DOI: 10.1109/ACCESS.2025.3579919	M21
12	**Mihaljević, M. J.**, Kavčić, A., Matsuura, K., "An Encryption Technique for Provably Secure Transmission from a High Performance Computing Entity to a Tiny One", *Mathematical Problems in Engineering*, vol. 2016, Article ID 7920495, pp. 1-10, DOI: 10.1155/2016/7920495.	M22
13	**Mihaljević, M. J.**, Oggier, F., "Security evaluation and design elements for a class	M22

	of randomised encryptions", *IET Information Security*, vol. 13(1) (2019), pp. 36-47, DOI: 10.1049/iet-ifs.2017.0271.	
14	**Mihaljević, M. J.**, Wang, L., Xu, S., "An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors", *Entropy*, vol. 24(3) (2022), 406, DOI: 10.3390/e24030406	M22
15	**Mihaljević, M. J.**, "A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off", *IEEE Access*, vol. 8, 2020, pp. 141258–141268, DOI: 10.1109/ACCESS.2020.3013199	M21a
16	**Mihaljević, M. J.**, Knežević, M., Urošević, D., Wang, L., Xu, S., "An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT", *Symmetry*, vol. 15(2) (2023), 299, DOI: 10.3390/sym15020299	M21
17	**Mihaljević, M. J.**, Wang, L., Xu, S., Todorović, M., "An Approach for Blockchain Pool Mining Employing the Consensus Protocol Robust Against Block Withholding and Selfish Mining Attacks", *Symmetry*, vol. 14(8) (2022), 1711, DOI: 10.3390/sym14081711	M21
18	**Mihaljević, M. J.**, Todorović, M., Knežević, M., "An Evaluation of Power Consumption Gain and Security of Flexible Green Pool Mining in Public Blockchain Systems", *Symmetry*, vol. 15(4) (2023), 924, DOI: 10.3390/sym15040924	M21
19	Wang, Q., Wang, L., Xu, S., Zhang, S., Shao, W., **Mihaljević, M. J.**, "Single-Layer Trainable Neural Network for Secure Inference", *IEEE Internet of Things Journal*, vol. 12(3), pp. 2968-2978, 2025, doi:10.1109/JIOT.2024.3480195.	M21a+
20	Xu, S., Dong, S., Wang, L., **Mihaljević, M. J.**, Zhang, S., Shao, W., & Wang, Q. "Blockchain-based Secure Data Sharing with Overlapping Clustering and Searchable Encryption", *Computer Standards & Interfaces*, vol. 93, 2025, 103979, DOI: 10.1016/j.csi.2025.103979	M21a
21	Xu, S., Zhang, L., Wang, L., **Mihaljević, M. J.**, Zhang, S., Shao, W., & Wang, Q. "Relay Network-based Cross-chain Data Interaction Protocol with Integrity Audit", *Computers and Electrical Engineering*, vol. 117, 2024, 109262, DOI: 10.1016/j.compeleceng.2024.109262	M21
22	Xu, S., Wang, Z., Wang, L., **Mihaljević, M. J.**, Zhang, S., Shao, W., Wang, Q., "A sharding scheme based on graph partitioning algorithm for public blockchain", *Computer Modeling in Engineering & Sciences*, vol. 139(3), pp. 3311-3327, 2024, doi:10.32604/cmes.2023.046164.	M21
23	Xu, S., He, H., **Mihaljević, M. J.**, Zhang, S., Shao, W., Wang, Q., "DBC-MulBiLSTM: A DistilBERT-CNN Feature Fusion Framework enhanced by multi-head self-attention and BiLSTM for smart contract vulnerability detection", *Computers and Electrical Engineering*, vol. 123, 110096, 2025, doi:10.1016/j.compeleceng.2025.110096.	M21
24	Zhang, S., Hu, C., Wang, L., **Mihaljević, M. J.**, Xu, S., & Lan, T. "A Malware Detection Approach Based on Deep Learning and Memory Forensics", *Symmetry*, vol. 15(3), 2023, 758, DOI: 10.3390/sym15030758	M21

V.3 Услови дефинисани за ментора у складу са *Правилима докторских студија Универзитета у Новом Саду* за област којој припада докторска дисертација:

На основу Закона о високом образовању, као и у складу са Правилима докторских студија Универзитета у Новом Саду, која су усвојена на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, и која су ступила на снагу 5.3.2021., а примењују се од 1.4.2021. године (Измене и допуне: 27.10.2022. године; 30.3.2023. године; 28.3.2024. године и 30.9.2025. године) и према Правилнику о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности Факултета техничких наука (број 01-195/11-1) од 7.10.2021. године, ментор је по правилу наставник датог студијског програма, који поред услова, који су дефинисани стандардима за акредитацију, има најмање пет радова који су публиковани у часописима са импакт фактором са SCI листе, односно SCIe листе у претходних 10 година.

Образложење: **Комисија закључује да др Миодраг Ј. Михаљевић испуњава услове дефинисане за ментора у складу са Правилима докторских студија Универзитета у Новом Саду и оцењује се као ПОДОБАН за ментора на изради докторске дисертације кандидата.**
Да ли ментор испуњава услове? ДА

VI ЗАКЉУЧАК

Тема је подобна	**ДА**
Кандидат је подобан	**ДА**
Ментор је подобан	**ДА**

Образложење о подобности теме, кандидата и ментора (до 500 речи):

Комисија је детаљно проучила достављену пријаву кандидата, проценила значај наведених референци везаних за тему истраживања, референце предложеног ментора и кандидата, као и њихове досадашње резултате у наведеној области истраживања. На основу чињеница наведених у овом Извештају, Комисија закључује следеће:

- предложена тема је подобна за докторску дисертацију — тема је актуелна, научно оправдана и добро дефинисана;
- предложено истраживање, хипотезе, циљеви, методологија и очекивани резултати истраживања су добро осмишљени и одговарајући за израду докторске дисертације;
- кандидат Синиша Томовић, мастер математичар, подобан је за израду предложене докторске дисертације;
- др Миодраг Ј. Михаљевић, научни саветник на Математичком институту САНУ и дописни члан САНУ, изабран 2021. године, подобан је за ментора предложене докторске дисертације.

На основу наведених закључака, Комисија предлаже Наставно-научном већу Факултета техничких наука у Новом Саду и органима Универзитета у Новом Саду да прихвате тему за израду докторске дисертације под насловом „Дизајн и напади на класу RFID аутентификационих протокола чија је сигурност заснована на тешком LPN проблему“ (Design and attacks on a class of RFID authentication protocols whose security is based on the hard LPN problem) кандидата Синише Томовића и да се као ментор именује др Миодраг Ј. Михаљевић, научни саветник на Математичком институту САНУ и дописни члан САНУ.

Место и датум:

Нови Сад, Београд, 7.5.2026.

1. др Зоран Огњановић, научни саветник_____, председник

2. др Силвиа Гилезан, редовни професор_____, члан

3. др Филип Марић, редовни професор_____, члан

4. др Драган Урошевић, редовни професор_____, члан

5. др Горан Сладић, редовни професор_____, члан

6. др Бранко Милосављевић, редовни професор_____, члан

НАПОМЕНА: *Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај и да исти потпише.*