# Analiza metoda u lakoj kriptografiji

Nataša Dimić, Prof. Dr. Mirjana Radivojević [1]

***Sadržaj –*** **Najnoviji izveštaji i Internet statistike predviđaju da će broj uređaja povezanih na IP mreže biti više od tri puta veći od globalne populacije do kraja 2022. godine. Porast broja uređaja usko je povezan sa pomacima u industriji i razvojem mobilnih komunikacionih sistema, kao i enormnim porastom broja mobilnih korisnika praćenim razvojem 5G mreža i tehnologije Interneta stvari (*IoT - Internet of Things*). Međutim, sa tehnološkim napretkom na polju Interneta stvari (*IoT*), u upotrebi je sve više uređaja koji nemaju na raspolaganju dovoljno resursa za izvršavanje složenih algoritama, a zahtevaju određeni stepen zaštite podataka koje razmenjuju. Laka kriptografija (*Lightweight Cryptography*) je tehnologija koja ima za cilj da takvim uređajima obezbedi sigurnu komunikaciju, imajući u vidu ograničenu snagu, procesorske i memorijske resurse. Prema osnovnoj definiciji, laka kriptografija je kriptografski algoritam ili protokol skrojen za primenu u ograničenim okruženjima, koji proširuje primenu kriptografije na ograničene uređaje (uključujući *RFID* čipove, senzore, beskontaktne pametne kartice, zdravstvene i slične uređaje). Međunarodna standardizacija i prikupljanje smernica za dalji razvoj ove oblasti su trenutno u toku.**

**Cilj master rada je dvojak. Sa jedne strane, u radu su predstavljeni teorijski koncepti, algoritmi i protokoli vezani za implementaciju zaštite i sigurnosnih protokola u Internetu stvari. Dat je pregled do sada predloženih standarda, uključujući grupu *ISO/IEC JTC 1/SC 27* i standard *ISO/IEC 29192,* koji je najnoviji projekat u procesu standardizacije. U radu su razmatrane hardverske i softverske karakteristike sistema koje uslovljavaju implementaciju lake kriptografije, kao što su arhitektura čipa, veličina *RAM* memorije, veličina implementacije algoritma i potrošnja energije. Sa druge strane, u radu je predstavljeno nekoliko različitih metoda za primenu lake kriptografije koje uključuju različite pristupe i koje su do sada privukle najveću pažnju stručne javnosti. Objašnjen je način rada i primena svake metode. Zatim su analizirani potrebni resursi i performanse metoda na različitim mikrokontrolerima koji**

[1] Nataša Dimić, Računarski fakultet, Univerzitet Union, Knez Mihailova 6/6, Beograd, Srbija
(e-mail: natasa.dimic@gmail.com)
Prof. Dr. Mirjana Radivojević, Računarski fakultet, Univerzitet Union, Knez Mihailova 6/6, Beograd, Srbija
(e-mail: mradivojevic@raf.rs)

**simuliraju rad mikroprocesora u tehnologiji Interneta stvari, a rezultati su upoređeni u tabelama. Konačno, razmotreni su nedostaci ovih metoda i potencijalni napadi, kao i buduća primena i dalji razvoj lake kriptografije u okviru tehnologije Interneta stvari.**

***Ključne reči*** **– Internet stvari, 5G *IoT*, Laka kriptografija, Metode lake kriptografije, Blok šifre, Strim šifre, Heš funkcije, Digitalni potpisi, *SIMON, SPECK, CHACHA, TRIVIUM, PHOTON, SPONGENT, CHASKEY, FELICS***

## I. UVOD

Pojava prvih računara čini prekretnicu u razvoju kriptografskih algoritama. Sa porastom kompleksnosti mikroprocesora i njihovog radnog kapaciteta, povećavala se i moguća složenost kriptografskih algoritama koji se mogu izvršavati u realnom vremenu. Međutim, ovaj napredak u snazi procesiranja je doprineo i povećanju broja sofisticiranih kriptoanalitičkih alata. Stoga se može reći da istorija moderne kriptografije u prethodnih nekoliko decenija predstavlja stalnu borbu između kriptografa i kriptoanalitičara, gde obe strane imaju pristup tehnologiji koja napreduje velikom brzinom.

Najpouzdanije metode za enkripciju i autentifikaciju koje se danas koriste zahtevaju određenu procesorsku snagu, raspoloživu memoriju i određenu količinu energije na uređajima na kojima se izvršavaju. Sa tehnološkim napretkom na polju Interneta stvari (*IoT*), u upotrebi je sve više uređaja koji nemaju na raspolaganju dovoljno resursa za izvršavanje složenih algoritama, a zahtevaju određeni stepen zaštite podataka koje razmenjuju. Laka kriptografija (*Lightweight Cryptography*) je tehnologija koja ima za cilj da takvim uređajima obezbedi sigurnu komunikaciju, imajući u vidu ograničenu snagu, procesorske i memorijske resurse.

U prethodne dve decenije je učinjen veliki pomak u oblasti lake kriptografije, kada su u pitanju dizajn i optimizacija novih. Objavljena su brojna istraživanja koja se bave kriptoanalizom, testiranjem sigurnosti i analizom performansi kriptografskih metoda. Sa druge strane, u domaćim istraživanjima, laka kriptografija je i dalje nova oblast. Cilj ovog rada je analiza metoda lake kriptografije, koja pre svega obuhvata pregled stanja u ovoj oblasti, osnovnih teorijskih koncepta i procesa standardizacije metoda, a zatim i pregled kriptografskih metoda koje se uspešno primenjuju u današnjim *IoT* uređajima, kao i poređenje njihovih performansi na uređajima sa ograničenim resursima.

## II. INTERNET STVARI I POTREBA ZA LAKOM KRIPTOGRAFIJOM

Internet stvari (eng. *Internet of Things*, skraćeno *IoT*) predstavlja sistem objekata koji su međusobno povezani i razmenjuju podatke putem telekomunikacione mreže. Pojam Interneta stvari je definisan u okviru Inicijative globalnih standarda (eng. *Global Standards Initiative*, skraćeno *GSI*) [1] 2012. godine, dok su koncept i sam termin aktuelni već najmanje četiri decenije, od 1982. godine kada je prvi automat za prodaju pića povezan na *ARPANET* mrežu [2]. Stvari u okviru tehnologije Interneta stvari obuhvataju fizičke uređaje i virtuelne objekte (softver) koji mogu da se identifikuju i povežu u komunikacionu mrežu. U prvim definicijama Interneta stvari, pojam stvari se odnosi na *RFID* tagove (eng. *Radio-Frequency Identification*, skraćeno *RFID*) [7], male objekte koji primaju i šalju podatke putem radio talasa.

U zavisnosti od namene, uređaji u okviru Interneta stvari pored sposobnosti da međusobno komuniciraju, mogu da imaju i druge funkcionalnosti, kao što su registrovanje događaja, prikupljanje, skladištenje i prosleđivanje podataka. Takođe, neki uređaji mogu da izvršavaju određene operacije, u skladu sa prikupljenim ili primljenim informacijama. Sa druge strane, softver u tehnologiji Interneta stvari predstavlja aplikacije za različite inteligentne sisteme, koji takođe mogu da prikupljaju, procesiraju i prosleđuju informacije drugim stvarima na mreži. Komunikacija i razmena podataka ostvaruje se komunikacionim medijumima zasnovanim na *TCP/IP* protokolu, koji uključuju žičanu infrastrukturu, bežične, mobilne, satelitske mreže, blutut (eng. *bluetooth*), komunikaciju kratkog polja (eng. *Near Field Communication*, skraćeno *NFC*), komunikaciju putem radio talasa (*RFID*), kao i mreže nove generacije (eng. *New Generation Networks*, skraćeno *NGN*).

Veliki napredak u industriji i tehnologijama komunikacionih mreža prethodnih decenija direktno je uticao na porast broja uređaja u Internetu stvari. Razvoj mobilnih mreža je doprineo sve većem broju mobilnih korisnika, a dosadašnji kao i budući razvoj 5G mreža igra značajnu ulogu u sve većem broju međusobno povezanih uređaja. Izuzetno važan aspekt u komunikaciji i razmeni informacija između ovih uređaja je sigurnost, i to mogućnost autentifikacije, očuvanja privatnosti i bezbedne razmene velike količine informacija u okviru sistema koji obuhvata uređaje različitih performansi, kapaciteta i protokola za komunikaciju. Uspostavljanje sigurne komunikacije u raznolikom sistemu Interneta stvari je osnovni zadatak kriptografskih metoda, čiji dizajn mora da bude prilagođen ograničenim resursima *IoT* uređaja.

A. Porast broja *IoT* uređaja

Brojna istraživanja i analize su se bavile otkrivanjem i predviđanjem trendova porasta broja korisnika komunikacionih usluga (Internet, mobilne mreže), kao i porasta broja *IoT* uređaja. Prema izveštaju koji je objavio *Cisco*, koji obuhvata kvantitativnu i kvalitativnu analizu i predviđanje korišćenja i performansi mreža na globalnom nivou [3], broj uređaja povezanih na *IP* mreže će biti više od tri puta veći od globalne populacije do kraja 2022. godine, dok će do kraja 2023. godine iznositi 29.3 milijardi uređaja. Predviđeno je da će polovinu ovih konekcija, tj. 14.7 milijardi, činiti mašina-mašina (eng. *Machine-To-Machine*, skraćeno *M2M*) konekcije, dok će skoro polovina konekcija u ovoj kategoriji pripadati kućnim *IoT* uređajima. Drugu najveću kategoriju povezanih uređaja u predikciji čine pametni telefoni. Na slici 1 je dato poređenje broja uređaja povezanih na *IP* mreže od 2018. do 2023. godine.


Slika 1 Porast broja uređaja i konekcija, *Cisco* godišnji izveštaj [3]

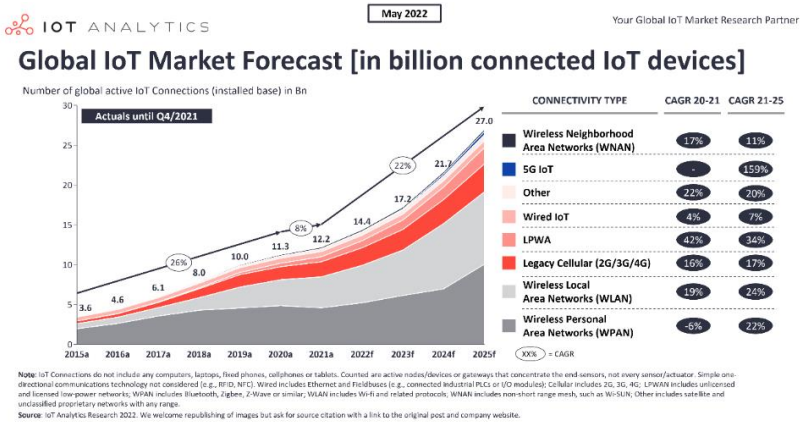
Kompanija *IT Analytics*, vodeća u istraživanju tržišta Interneta stvari i Industrije 4.0, predvidela je eksponencijalni porast broja *IoT* konekcija u narednih nekoliko godina, uz očekivanje da će 2022. godine broj *IoT* konekcija premašiti 14.4 milijardi [4]. Na slici 2 je dat prikaz rezultata ovog istraživanja, gde su ustanovljeni stvarni (a – eng. *actual*) i predviđeni (f – eng. *forecast*) brojevi podeljeni prema vrsti konekcije.

Postoji više faktora koji utiču na brzinu porasta broja konekcija i *IoT* uređaja. Niže cene i naprednije tehnologije hardverskih komponenti koje su ključne u tehnologiji Interneta stvari, kao što su senzori, procesori i memorije, su podstakle veću primenu ove tehnologije. Senzori prikupljaju i generišu informacije iz svog okruženja, i imaju široku primenu u *IoT* svetu. Procesori

obrađuju prikupljene podatke i generišu novo znanje na osnovu dobijenih informacija i definisanih algoritama obrade, dok memorijske komponente skladište podatke. Razvoj računarstva u oblaku, nauke o podacima, mašinskog učenja i naprednih tehnologija kod računarskih i mobilnih mreža se pozitivno odrazio na porast broja *IoT* konekcija, kao i društveni faktor, konzumerizam i velika potražnja koji podstiču sve veću proizvodnju *IoT* uređaja.

Na slici 2 je primetno usporenje porasta utvrđenog broja *IoT* konekcija u najtežem periodu globalne pandemije COVID-19, koja je prouzrokovala poremećaj u proizvodnji, transportu, isporučivanju resursa, pa samim tim i nestašici čipova. Sa druge strane, ovim istraživanjem je ustanovljeno i da je pandemija imala pozitivan uticaj na brže usvajanje i veću potražnju za *IoT* tehnologijama. Nemogućnost putovanja i direktnog kontakta je podstakla ljude i kompanije da komunikaciju ostvare putem Interneta, povezujući se i razmenjujući informacije pomoću pametnih uređaja. Očekuje se da će pandemija i dalje imati značajan uticaj na razvoj *IoT* tržišta, kao i inflacija i političko-ekonomska kriza, koji negativno utiču na isporučivanje resursa za proizvodnju čipova. Veliki izazov za kompanije predstavlja i nedostatak stručnjaka u oblastima digitalne transformacije, veštačke inteligencije, Interneta stvari i računarstva u oblaku.

Porast broja *IoT* uređaja dovodi do povećanja Internet saobraćaja, količine podataka, kao i potrebnog smeštajnog prostora, procesorske snage i mrežnog kapaciteta. Potreba za bržim i pouzdanim kanalima komunikacije je pokretač daljeg razvoja tehnologija telekomunikacionih sistema.




Slika 2 Porast broja aktivnih *IoT* konekcija, *IT Analytics* [4]

B. Uticaj razvoja 5G mreža na *IoT*

5G je skraćenica za petu generaciju mobilnih mreža, koja koristi širi opseg frekvencija, što omogućava veću brzinu prenosa podataka i opsluživanje daleko većeg broja uređaja. Najveća brzina prenosa podataka postiže se na visokim frekvencijama (*mmWave*) koje obuhvataju deo spektra od 24 – 100 GHz. Međutim, signal na ovim frekvencijama ima kratak domet i osetljiv je na prepreke. Na srednjim i nižim frekvencijama koje obuhvataju deo spektra od 1 – 6 GHz, odnosno deo spektra ispod 1 GHz, postiže se bolji domet i niža brzina prenosa. Da bi se postigle optimalne performanse kako u gusto naseljenim gradovima, gde je potrebno povezati veliki broj uređaja, tako i u ruralnim slabo naseljenim predelima, gde je potreban veći domet, 5G mreže koriste sva tri dela spektra u zavisnosti od potrebe [5].

5G mreže se smatraju ključnom za razvoj Interneta stvari upravo zbog većeg propusnog opsega, bržeg prenosa podataka, bržeg odziva i mogućnosti povezivanja većeg broja uređaja. Pored toga, kod 5G mreža se predviđa bolja pokrivenost, što bi poboljšalo povezivanje uređaja u okviru pametnih gradova, pametnih kuća i transporta [7]. U poređenju sa 4G mrežama, 5G mreže znatno smanjuju potrošnju energije uređaja [6]. S obzirom na to da neki *IoT* uređaji koji se napajaju isključivo baterijama mogu da budu postavljeni na udaljenim, nepristupačnim lokacijama, zadatak tehnologija primenjenih u Internetu stvari, što uključuje i 5G, jeste da smanji potrošnju i produži životni vek baterija [7]. Konačno, 5G mreže pružaju otpornost, bezbednu komunikaciju, identifikaciju i autentifikaciju, očuvanje integriteta i privatnosti podataka, i nastavljaju da se razvijaju u skladu sa najvišim sigurnosnim standardima [8].

Iako nova generacija mobilnih mreža još uvek nije dovoljno rasprostranjena, brojna istraživanja se bave uticajem ove tehnologije na budući razvoj telekomunikacija, industrije i biznisa. 5G će omogućiti razvoj novih aplikacija u skladu sa boljim performansama, modernu arhitekturu u povezivanju *IoT* uređaja, kao i prelazak na platforme bazirane na računarstvu u oblaku [9].

C. Sigurnost IoT uređaja

Internet stvari je heterogen sistem uređaja i aplikacija koji razmenjuju veliku količinu osetljivih informacija, prikupljenih u industriji, poljoprivredi, transportu, zdravstvu, vojsci, kao i ličnih podataka ljudi, koji otkrivaju njihovo kretanje i aktivnosti. Veliki izazov u očuvanju privatnosti, autentičnosti i integriteta podataka predstavlja integrisanje različitih sigurnosnih polisa i tehnologija. Da bi *IoT* tehnologija nastavila globalnu ekspanziju, svaki korak u toku podataka, uključujući prikupljanje, skladištenje, obradu i prenos, zahteva visok stepen zaštite od napada i neovlašćenog pristupa.

*IoT* uređaji često nisu pod stalnim fizičkim nadzorom i izloženi su fizičkim napadima i neovlašćenom pristupu, dok komunikacija bežičnim mrežama dovodi do rizika od prisluškivanja [10]. Kod *RFID* tagova i senzora je poznat problem autentifikacije, gde su komponente sistema podložne napadu čovek-u-sredini (eng. *Man-in-the-middle attack*, skraćeno *MITM*) [10], dok neki *IoT* uređaji ne vrše autentifikaciju i takođe podležu ovoj vrsti napada [11]. Takođe, rad uređaja i aplikacija je moguće poremetiti slanjem ogromne količine zahteva ili otvaranjem velikog broja konekcija koje *IoT* komponenta ne može da obradi i time ne može da opsluži ni validne zahteve (eng. *Denial Of Service attack*, skraćeno *DoS*, ili eng. *Distributed Denial of Service attack*, skraćeno *DDoS*) [11]. Da bi se sprečili *MIMT, DoS* i drugi napadi, potrebno je preduzeti mere prevencije i zaštite sistema, koji uključuju sisteme za detekciju upada (eng. *Intrusion Detection Systems*, skraćeno *IDS*), antivirus softver, ispravnu autentifikaciju, enkripciju, fizičku zaštitu, kao i edukaciju korisnika na temu bezbednosti na Internetu.

Veliki broj *IoT* uređaja ima ograničen memorijski prostor, procesorsku snagu i napajanje, što ograničava izvršavanje složenih algoritama koji se danas pouzdano koriste u zaštiti računarskih sistema. Stoga se javlja potreba za razvojem novih, lakših metoda koje pružaju dobar stepen zaštite uprkos ograničenim raspoloživim resursima.

## III. LAKA KRIPTOGRAFIJA

Laka kriptografija (eng. *Lightweight Cryptography*, skraćeno *LWC*) predstavlja kriptografske algoritme i protokole koji su namenjeni uređajima sa ograničenim resursima. Ovi uređaji pre svega obuhvataju uređaje u okviru Interneta stvari, kao što su *RFID* čipovi, senzori, beskontaktne pametne kartice, pametni uređaji u domaćinstvima, industriji, zdravstvu i drugi. Usled porasta broja *IoT* uređaja, uvedeni su međunarodni standardi i definisani zahtevi koje algoritmi moraju da ispune da bi se smatrali lakim. Nacionalni Institut Standarda i Tehnologije (eng. *National Institute of Standards and Technology*, skraćeno *NIST*) je otvorio projekat na temu lake kriptografije 2013. godine [12][13] i objavio poziv za prijavu metoda 2018. godine [13], sa ciljem definisanja standarda i određivanja metoda koje pružaju dobre performanse i zaštitu na uređajima sa ograničenim resursima. Takođe, grupa *ISO/IEC JTC 1/SC 27* udruženog tehničkog komiteta (eng. *Joint Technical Committee*, skraćeno *JTC*) Međunardone organizacije za standardizaciju (eng. *International Organization for Standardization*, skraćeno *ISO*) i Međunarodne elektrotehničke komisije (eng. *International Electrotechnical Commission*, skraćeno *IEC*) razvija međunarodne standarde, tehničke specifikacije i

izveštaje u oblasti informacione bezbednosti, bezbednosti na Internetu i zaštite privatnosti. Prema *ISO* izveštaju, trenutno postoji preko 200 objavljenih standarda i preko 60 koji su u razvoju [14]. Objavljeni standardi uključuju i standard *ISO/IEC 29192* koji se odnosi na standardizaciju lake kriptografije.

*ISO/IEC 29192* [15] je projekat koji se odnosi na pojmove i definicije u oblasti lake kriptografije, kao i sigurnosne i implementacione kriterijume namenjene metodama lake kriptografije. Ovaj standard je objavljen 2012. godine sa opštim definicijama, a danas sadrži osam sekcija, koje obuhvataju standardizaciju blok i strim šifri, heš funkcija i metoda autentifikacije.

Pojam lake kriptografije trenutno nije rasprostranjen u srpskom jeziku. Prema predlogu plana donošenja srpskih standarda za 2018. godinu *prSRPS ISO/IEC 29192-1:2018* Instituta za standardizaciju Srbije, predložen je prevod "lagana kriptografija" [16] u okviru projekta *ISO/IEC 29192*, dok je u objavljenom standardu *SRPS ISO/IEC 29192-2:2020* iz 2020. godine koji je zamenio pomenuti predlog, upotrebljen prevod "laka kriptografija" [17]. U ovom radu je korišćen prevod prema objavljenom standardu iz 2020. godine.

*ISO/IEC 29167-21* [18] i *ISO/IEC 29167-22* [19] su standardi koji se odnose na upotrebu i implementaciju *SIMON* i *SPECK* metoda kod *RFID* uređaja, u okviru projekta automatske identifikacije i tehnika prikupljanja podataka.

*ETSI EN 303 645* [20] je međunarodni standard objavljen 2020. godine, koji se odnosi na bezbednost i privatnost *IoT* uređaja, kada je u pitanju upravljanje osetljivim podacima u skladu sa evropskom regulativom o zaštiti podataka (eng. *General Data Protection Regulation*, skraćeno *GDPR*).

### A. Dosadašnja istraživanja u oblasti lake kriptografije u Srbiji

U procesu standardizacije metoda lake kriptografije u Srbiji, usvojen je termin lake kriptografije za kriptografske algoritme namenjene uređajima sa ograničenim resursima. Oblast lake kriptografije još uvek nije zastupljena u domaćoj naučnoj zajednici. Dosadašnja istraživanja obuhvataju pregled blok šifri za upotrebu u bežičnim senzorskim mrežama [38], kao i analizu lakih kriptografskih protokola za primenu u preciznoj poljoprivredi [39]. U skladu sa javno dostupnim istraživanjima i objavljenim radovima zaključno sa februarom 2023. godine, ovaj rad predstavlja prvu sveobuhvatnu analizu metoda lake kriptografije u domaćim istraživanjima.

### B. Kriterijumi lake kriptografije

Metode lake kriptografije moraju da ispunjavaju određene kriterijume da bi mogle efikasno da se izvršavaju na *IoT* uređajima sa ograničenim resursima [21]. Potrebno je uzeti u obzir sledeće parametre:

- veličina – veličina čipa i raspoložive *ROM/RAM* memorije određuju dozvoljenu veličinu implementacije kriptografskog algoritma i memoriju koju ima na raspolaganju za svoje izvršavanje;
- snaga – snaga uređaja određuje složenost algoritma koji može da se efikasno izvršava; snaga zavisi od procesora koji uređaj poseduje, pa se kao kriterijum snage uređaja posmatra veličina čipa; ovaj parametar je izuzetno važan kod uređaja koji se napajaju iz svog okruženja, kao što su *RFID* čipovi koji koriste elektromagnetno polje čitača za napajanje svog električnog kola.
- potrošnja energije – utrošena energija prilikom izvršavanja kriptografskog algoritma ograničava implementaciju na uređajima koji se napajaju baterijama; s obzirom na to da količina utrošene energije zavisi od brzine procesiranja, brzina se uzima kao kriterijum prilikom klasifikacije kriptografskih metoda;
- brzina procesiranja – kod brzine procesiranja se razmatraju protok i kašnjenje; protok je ključan faktor kod uređaja koji procesiraju veliku količinu podataka, kao što su kamere, dok je kašnjenje ključno kod uređaja koji moraju da se odazivaju u realnom vremenu, kao što su sistemi za kontrolu i nadzor.

Pored navedenih kriterijuma, metode lake kriptografije moraju da obezbede zadovoljavajući stepen zaštite. Kod uređaja sa ograničenim resursima je potrebno pronaći kompromis između složenosti algoritma i dužine ključa, koji određuju sigurnost algoritma, i potrošnje raspoloživih resursa uređaja, kako bi se algoritam uspešno izvršavao bez ometanja rada samog uređaja. U zavisnosti od tipa uređaja, kriptografske metode mogu da budu implementirane hardverski i softverski, čime određeni kriterijumi dobijaju na važnosti.

### C. Hardverska implementacija

Hardverska implementacija algoritma podrazumeva dizajniranje električnog kola na čipovima pomoću logičkih elemenata. Kod kriptografskih algoritama, posmatra se površina obuhvaćenih logičkih elemenata implementacijom algoritma. Kod programabilnih integrisanih kola (eng. *Field-Programmable Gate Array*, skraćeno *FPGA*) se posmatraju rekonfigurabilne jedinice koje obuhvataju logičke elemente, multipleksere i lukap (eng. *look-up*) tabele, dok se kod integrisanih kola specifične namene (eng. *Application-specific integrated circuit*, skraćeno *ASIC*) posmatraju jedinice izvedene iz veličine jednog dvoulaznog *NI* (*NAND*) logičkog elementa (eng. *Gate Equivalent*, skraćeno *GE*) [12]. Manja implementacija algoritma znači i manju potrošnju energije za svoje izvršavanje, dok se paralelizacija, a samim tim i bolji protok i manje kašnjenje, postižu uz pomoć više logičkih elemenata na većoj površini.

Hardversku implementaciju algoritma je potrebno prilagoditi i raspoloživoj memoriji čipa. Razmatraju se proizvodi kalkulacije koji se smeštaju u memoriju uređaja, kao i veličina ključa i veličina bloka koji se obrađuje, imajući u vidu da ovi parametri direktno utiču na sigurnost algoritma [23].

### D. Softverska implementacija

Softverska implementacija podrazumeva izvršavanje algoritma u okviru programskog koda koji je smešten u memoriji i izvršava se uz pomoć procesora. Kod implementacije algoritma važna je veličina koda koji zauzima memoriju uređaja (*ROM* memorija), kao i potrošnja memorije za izvršavanje kalkulacija (*RAM* memorija) [12]. Posmatra se i protok, tj. brzina izvršavanja [23]. Kod softverskih implementacija kriptografskih algoritama, poželjna je manja potrošnja memorije i brže izvršavanje, što je potrebno postići usklađivanjem parametara u skladu sa potrebama i resursima uređaja.

## IV. METODE LAKE KRIPTOGRAFIJE

U prvom krugu evaluacije kriptografskih algoritama, *NIST* [13] je razmotrio 56 kandidata, od kojih je 32 prihvaćeno za drugi krug evaluacije, gde su razmotreni dokazi o bezbednosti algoritama, kao i njihove performanse na uređajima sa ograničenim resursima. Postavljene kriterijume je ispunilo 10 kandidata. Ovakav projekat je omogućio detaljno istraživanje kriptografskih algoritama, njihove podložnosti pojedinim napadima, ispitivanje performansi, kao i utvrđivanje potencijala za dalji napredak. Sa druge strane, *ISO/IEC* standardizacija u okviru projekta *ISO/IEC 29192* [15] do sada definiše 11 algoritama koji su pogodni za primenu u lakoj kriptografiji.

Metode lake kriptografije se okvirno grupišu u blok (eng. *block ciphers*) i strim (eng. *stream ciphers*) šifre, heš (eng. *hash*) funkcije i kodove za autentifikaciju poruka (eng. *Message Authentication Codes*, skraćeno *MAC*). Blok i strim metode se obično koriste za enkripciju/dekripciju podataka, dok se heš funkcije i *MAC* algoritmi koriste za proveru integriteta podataka i autentifikaciju.

### A. Blok šifre

Blok šifre (eng. *block ciphers*) predstavljaju determinističke algoritme koji obrađuju ulazni podatak u blokovima specificirane veličine. Preciznije rečeno, blok metode za isti ulazni podatak uvek generišu isti rezultat. Blok metode se koriste i za kreiranje drugih vrsta kriptografskih algoritama, kao što su strim metode, heš funkcije i generatori pseudoslučajnih brojeva. Standard za enkripciju *AES* (eng. *Advanced Encryption Standard*) pripada blok metodama,

kao i metode lake kriptografije *PRESENT*, *CLEFIA* i *LEA*, koje su prihvaćene u okviru standarda *ISO/IEC 29192* [15], zatim *RC5*, *SIMON*, *SPECK* i druge.

*SIMON* i *SPECK* metode je objavila Nacionalna Bezbednosna Agencija (eng. *National Security Agency*, skraćeno *NSA*) u Sjedinjenim Američkim Državama 2013. godine, sa ciljem da obezbedi protokol koji na uređajima Interneta stvari ima dobre performanse i zadovoljavajući stepen zaštite [25]. *SIMON* je optimizovan na hardverske, a *SPECK* za softverske implementacije. U radu sa *n*-bitnim rečima, koriste blokove veličine *2n* bita, i ključeve veličine *m* reči, što predstavlja *mn* bita. U skladu sa određenom veličinom bloka i ključa, određena implementacija metoda se obeležava sa *SIMON 2n/mn* i *SPECK 2n/mn*. Do sada su brojna istraživanja pokazala da implementacije ovih metoda sa redukovanim brojem iteracija podležu napadima diferencijalne kriptoanalize, gde se analiziraju promene u originalnom tekstu i šifrovanom tekstu da bi se otkrio način rada algoritma šifrovanja i tajni ključ. Uprkos tome, *SIMON* i *SPECK* su standardizovani za primenu na *RFID* uređajima [18] [19] i odobreni za korišćenje na različitim *IoT* uređajima od strane *NSA*.

B. Strim šifre

Strim šifre (eng. *stream ciphers*) su kriptografski algoritmi koji uz pomoć pseudoslučajnog strima karaktera enkriptuju ulazne podatke sekvencijalno jedan po jedan bit ili bajt. Dizajnirane su po ugledu na enkripciju jednokratnim ključem, što predstavlja siguran način šifrovanja pod uslovom da je privatan ključ razmenjen na bezbedan način, a niz koji se generiše od ključa slučajan, bez ponavljanja i najmanje dužine kao i tekst koji se šifruje. Teorija korišćenja jednokratnog ključa u modernim telekomunikacionim sistemima potiče iz prve polovine 20. veka, a Klod Šenon je 1949. godine dokazao da u slučaju jednokratnih ključeva enkriptovana poruka ne odaje presretaču nikakve informacije o originalnoj poruci [26]. Strim šifre koriste kratak ključ, a niz koji se generiše je pseudoslučajan. Brze su i kod implementacije je kratak, što ih čini pogodnim za hardverske implementacije. Koriste se u uređajima i aplikacijama gde su ulazni podaci nepredvidive dužine. Za primenu u lakoj kriptografiji su standardizovane strim metode *Enocoro* i *Trivium* [15], a primeri drugih poznatih metoda su *ChaCha*, *Salsa20* i *RC4*.

ChaCha [28] metoda objavljena 2005. godine, srodna pseudoslučajnoj strim metodi *Salsa20* [27], od 256-bitnog ključa, 128-bitne konstante, 64-bitnog brojača i 64-bitnog jednokratnog broja (eng. *nonce*) primenom iterativnih operacija generiše 512-bitni strim ključa. Strim ključa se primenjuje u enkripciji ulaznog toka podataka. Zbog sigurnosti i dobrih performansi,

*ChaCha* metoda se koristi u *Google* aplikacijama, u operativnim sistemima i mobilnim uređajima, u hardverskim i softverskim implementacijama.

*Trivium* [29] je strim metoda objavljena u okviru *eSTREAM* projekta koji je završen 2008. godine [30]. Generiše maksimalno $2^{64}$-bitni strim ključa, koji se koristi za enkripciju ulaznog toka podataka. Istraživanja su pokazala mogućnost otkrivanja tajnog ključa kod implementacija sa umanjenim brojem iteracija, kao i teoretske napade u određenim implementacijama ove metode [31]. *Trivium* se koristi u *IoT* uređajima u pametnim kućama, pametnim satovima, medicinskim uređajima, industrijskim senzorima i kontrolnim sistemima. Zbog brzine, zauzeća male površine čipa i male potrošnje energije, namenjena je hardverskim implementacijama, ali postiže dobre performanse i u softverskim implementacijama.

C. Heš funkcije

Kriptografske heš funkcije su jednosmerne funkcije koje zadate podatke preslikavaju u niz karaktera određene dužine. Osobina jednosmernosti heš funkcija označava da ne postoji inverzna funkcija koja od generisane heš vrednosti izvodi originalne podatke. Heš funkcije su takođe deterministički algoritmi, to jest za isti ulaz uvek rezultuju istom izlaznom vrednošću. Heš vrednosti su jedinstvene, tačnije ne postoje dva različita ulazna podatka za koje heš funkcija generiše istu heš vrednost. Od heš funkcije se zahtevaju dobre performanse i dovoljan stepen sigurnosti, gde algoritam za malu promenu ulaznog podatka izračunava novu heš vrednost koja se toliko razlikuje od prethodne heš vrednosti, da je nemoguće utvrditi bilo kakvu korelaciju. Heš funkcije se koriste za utvrđivanje integriteta, kontrolne sume, skladištenje šifri, jedinstvenu identifikaciju objekata, autentifikaciju, konstruisanje *MAC* algoritama i algoritama digitalnog potpisivanja, kao i kod generatora pseudoslučajnih brojeva. Za primenu u lakoj kriptografiji standardizovane su metode *PHOTON*, *SPONGENT* i *Lesamanta-LW* [15].

*PHOTON* [32] i *SPONGENT* [33] metode su dizajnirane sa ciljem da unaprede performanse heš funkcija koje se koriste na *IoT* uređajima sa vrlo ograničenim resursima, kao što su *RFID* čipovi. Zasnovane su na principu rada "sunđer" funkcije (eng. *sponge function*) koja radi u fazama inicijalizacije, apsorbovanja i sažimanja, gde se primenom permutacije dobija heš vrednost tražene dužine. Operacija permutacije predstavlja primenu niza operacija nad matricom internog stanja. Zbog efikasne potrošnje procesorske snage, memorije i energije, obe metode su pogodne za hardverske implementacije, postižu visok stepen sigurnosti, koja se oslanja na veličinu ključa i složenost operacija, i imaju dobre performanse i u softverskim implementacijama.

### *D.* Digitalni potpisi i *MAC*

Digitalni potpisi su produkti asimetričnih matematičkih algoritama koji služe za utvrđivanje autentičnosti i integriteta podataka. Koriste se kada je potrebno sa sigurnošću potvrditi autora poruke ili dokumenta, i utvrditi da podaci u međuvremenu nisu izmenjeni. U procesu digitalnog potpisivanja poruke potpis se računa na osnovu sadžaja poruke i privatnog ključa autora, potpis se šifruje i šalje javnim kanalom zajedno sa porukom. Na strani primaoca se potpis dešifruje javnim ključem autora, i generiše novi potpis koji se poredi sa primljenim digitalnim potpisom. Kodovi za autentikaciju poruke (eng. *Message Authentication Codes*, skraćeno *MAC*) se takođe koriste za utvrđivanje autentičnosti i integriteta poruke. *MAC* kodovi predstavljaju kratku informaciju koja se generiše na osnovu deljenog privatnog ključa i poruke, i dodaju se poruci kao kontrolna vrednost. Za potrebe lake kriptografije su standardizovane *MAC* metode *LightMAC, Tsudik's keymode* i *Chaskey-12*.

Klasični *MAC* algoritmi *MD5, SHA-1* i *SHA-2* zasnovani na heš funkcijama, koriste velike blokove za enkripciju, što kod male količine podataka dovodi do neefikasne enkripcije, opterećenja registara i memorije uređaja. *MAC* algoritmi *AES* i *Triple-DES* zasnovani na blok šiframa su spori, opterećuju registre i memoriju računanjem ključeva iteracija. *Chaskey* [34] je *MAC* algoritam razvijen sa ciljem da prevaziđe probleme sa brzinom izvršavanja, potrošnjom energije i veličinom koda. Autori su matematički dokazali sigurnost *Chaskey* metode i predložili implementaciju od 16 iteracija, iako je utvrđeno da 8 iteracija pruža dovoljan stepen zaštite. Zbog sigurnosti i dobrih performansi *Chaskey* se koristi u raznim *IoT* uređajima, uključujući automobilsku industriju, kontrolne sisteme, platne kartice i sigurnosne protokole.

## V. Poređenje performansi

U prethodnoj deceniji metode lake kriptografije su bile predmet istraživanja i usavršavanja u naučnoj zajednici. U konkursu koji je organizovao *NIST* [13] bilo je potrebno utvrditi stepen sigurnosti prijavljenih metoda i izmeriti njihove performanse na uređajima sa ograničenim resursima. Parametri koji su ključni u merenju performansi metoda lake kriptografije su opisani u prethodnom poglavlju, i to u zavisnosti od tipa implementacije.

Za poređenje performansi hardverskih i softverskih implementacija kriptografskih metoda razvijene su platforme koje simuliraju rad algoritama na čipovima određene arhitekture i ograničenih resursa. Sprovedena su brojna istraživanja gde su upoređene različite implementacije metoda, na različitim mikrokontrolerima koji se koriste u uređajima Interneta stvari, korišćenjem

različitih metrika i parametara koji ocenjuju performanse algoritama. Takav način analize performansi otežava iznošenje bilo kakvih zaključaka na globalnom nivou kada su u pitanju sve objavljene metode lake kriptografije. U ovom trenutku je izvodljivo poređenje pojedinih metoda, gde je istraživanje sprovedeno na istom hardveru i u istim scenarijima simulacija.

Kod softverskih implementacija je postignut veći napredak u poređenju performansi kriptografskih algoritama. Platforma *FELICS* je osmišljena sa ciljem da prevaziđe pomenutu raznolikost u rezultatima istraživanja. Rezultati izvršavanja algoritama su dostupni za određene blok i strim metode, a platforma je dostupna za dalje korišćenje kako na postojećim, tako i na budućim kriptografskim metodama. U ovom radu su predstavljeni odabrani rezultati simulacija opisanih metoda lake kriptografije.

A. Performanse klasičnih kriptografskih metoda na *IoT* uređajima

*AES* (eng. *Advanced Encryption Standard*) je standard za enkripciju osetljivih podataka koji omogućava šifrovanje/dešifrovanje podataka korišćenjem simetričnog ključa. Primenjuje se u *IoT* uređajima, ali se ne smatra metodom lake kriptografije [37]. Predložene su lake verzije *AES* metode koje su optimizovane za rad na *IoT* uređajima. U poređenju sa standardizovanim metodama lake kriptografije, *AES* ima lošije performanse kada su u pitanju veličina koda, potrošnja memorije i brzina izvršavanja. Poređenjem performansi softverskih implementacija na platformi *FELICS* [36], ustanovljeno je da metode *SIMON*, *SPECK* i *Chaskey* imaju značajno manje veličine koda i zauzeće *RAM* memorije. *SIMON* i *SPECK* se izvršavaju brže u većini slučajeva u zavisnosti od mikrokontrolera, dok se *Chaskey* na svim korišćenim mikrokontrolerima izvršava višestruko puta brže od *AES* metode.

*SHA-256* (eng. *Secure Hash Algorithm*) pripada seriji *SHA-2* heš funkcija, koje su nasledile prethodnu seriju *SHA-1*. Proizvodi heš vrednosti veličine 256 bita i koristi se u mnogim aplikacijama i sigurnosnim protokolima. Kod uređaja sa ograničenim resursima, *SHA-256* nije idealan izbor zbog velikog iskorišćenja površine čipa. Prilikom analize metoda predloženih za heš funkcije u lakoj kriptografiji [33], hardverska implementacija metoda *SHA-256* je upoređena sa heš funkcijama *PHOTON* i *SPONGENT*, i ustanovljeno je da predložene metode za upotrebu u *IoT* uređajima zauzimaju približno dvostruko ili trostruko manju površinu, u zavisnosti od implementacije.

B. Performanse hardverskih implementacija

Kod određivanja performansi hardverskih implementacija kriptografskih algoritama koji se predlažu za korišćenje u lakoj kriptografiji, za hardversku

platformu se uzimaju čipovi koji imaju vrlo ograničene resurse, po ugledu na *RFID* čipove koji imaju slabo napajanje, integrisana kola male površine i malu raspoloživu memoriju. U dosadašnjim istraživanjima korišćeni su različiti *FPGA* i *ASIC* čipovi, i različite hardverske implementacije kriptografskih metoda, optimizovane za serijsko ili paralelizovano izvršavanje, što otežava poređenje performansi algoritama, s obzirom na to da ne postoji jedinstvena hardverska platforma za testiranje i poređenje svih metoda.

U specifikaciji metoda *SIMON* i *SPECK* [25], prikazane su performanse na *ASIC* čipovima napajanja 1.2 V i frekvencije 100 kHz. Rezultati su dati u tabeli 1 za različite veličine blokova i ključeva, kao i za dve vrste implementacija, od kojih je druga optimizovana za manju potrošnju površine čipa. Iz prikazanih rezultata se primećuje da *SIMON* metoda postiže bolje performanse od *SPECK* metode, što je u skladu sa njihovim inicijalnim namenama.

TABELA 1 PERFORMANSE HARDVERSKIH IMPLEMENTACIJA METODA *SIMON* I *SPECK*

| Metoda | Parametri | | Originalne implementacije | | Optimizovane implementacije | |
|---|---|---|---|---|---|---|
| | Blok [b] | Ključ [b] | Površina [GE] | Protok [kb/s] | Površina [GE] | Protok [kb/s] |
| SIMON | 48 | 96 | 763 | 15.0 | 739 | 5.0 |
| SPECK | 48 | 96 | 884 | 12.0 | 794 | 4.0 |
| SIMON | 64 | 96 | 838 | 17.8 | 809 | 4.4 |
| SPECK | 64 | 96 | 984 | 14.5 | 860 | 3.6 |
| SIMON | 64 | 128 | 1000 | 16.7 | 958 | 4.2 |
| SPECK | 64 | 128 | 1127 | 13.8 | 996 | 3.4 |
| SIMON | 96 | 96 | 984 | 14.8 | 955 | 3.7 |
| SPECK | 96 | 96 | 1134 | 13.8 | 1012 | 3.4 |
| SIMON | 128 | 128 | 1317 | 22.9 | 1234 | 2.9 |
| SPECK | 128 | 128 | 1396 | 12.1 | 1280 | 3.0 |

Autori *SPONGENT* algoritma su u svom radu [33] prikazali rezultate postignute hardverskim implementacijama heš funkcija na *ASIC* čipovima. U tabeli 2 su prikazani dobijeni rezultati za dve različite veličine heš vrednosti. Heš funkcija *SPONGENT* u zavisnosti od implementacije postiže manje iskorišćenje površine čipa, dok heš funkcija *PHOTON* postiže bolji protok.

TABELA 2 PERFORMANSE HARDVERSKIH IMPLEMENTACIJA HEŠ FUNKCIJA

| Metoda | Heš [b] | Površina [GE] | Protok [kb/s] |
|---|---|---|---|
| SPONGENT-128/128/8 | 128 | 1060 | 0.34 |
| SPONGENT-128/256/128 | 128 | 2641 | 0.68 |
| PHOTON-128/16/16 | 128 | 1122 | 1.61 |
| SPONGENT-256/256/16 | 256 | 1950 | 0.17 |
| SPONGENT-256/256/128 | 256 | 2641 | 0.68 |
| SPONGENT-256/512/256 | 256 | 5110 | 0.35 |
| PHOTON-256/32/32 | 256 | 2177 | 3.21 |

C. Performanse softverskih implementacija na *FELICS* platformi

*FELICS* (eng. *Fair Evaluation of Lightweight Cryptographic Systems*) [35] je platforma koja meri performanse softverskih implementacija metoda lake kriptografije na uređajima sa ograničenim resursima. Za razliku od prethodnih platformi koje koriste različite metrike i generišu rezultate evaluacije koji nisu lako uporedivi, *FELICS* je napisan sa ciljem da pruža fer poređenje i generiše konzistentne rezultate. Fer evaluacija se postiže predefinisanim kriterijumima koje implementacije metoda moraju da ispunjavaju.

Metode se izvršavaju na tri mikrokontrolera, koji prema arhitekturi i raspoloživim resursima odgovaraju integrisanim *IoT* uređajima. 8-bitni *AVR* mikrokontroler *ATmega128* je jedan od najboljih mikrokontrolera kada je u pitanju potrošnja energije, i koristi se u automatizaciji kod pametnih kuća, zgrada i u zdravstvenim uređajima. 16-bitni mikrokontroler *MSP430F1611* je jeftin, ima malu potrošnju energije i koristi se kod integrisanih aplikacija u industrijskim kontrolnim sistemima, senzorima i mernim uređajima. 32-bit *ARM Cortex-M3* je mikrokontroler visokih performansi dizajniran za uređaje ograničenog napajanja, koji se koriste u automobilima, industrijskim kontrolnim sistemima i bežičnim mrežama.

U *FELICS* platformi se razmatraju veličina koda, potrošnja memorije i vreme izvršavanja metoda. Snaga i potrošnja energije se ne mere u ovim simulacijama, jer je zaključeno da zavise i mogu se izvesti iz prethodna tri parametra. Rezultati simulacije softverskih implementacija odabranih metoda predstavljeni su u tabelama 3 i 4, za scenario prilagođen enkripciji i dekripciji kod komunikacije *IoT* uređaja, na sva tri mikrokontrolera. U slučaju blok šifri, najmanju veličinu koda ima *SPECK*, a najmanju potrošnju memorije i brzinu izvršavanja postiže *Chaskey*. U slučaju strim šifri, najmanju veličinu koda ima *ChaCha20* sa 128-bitnim ključem na svim mikrokontrolerima, najmanju potrošnju memorije postiže *Trivium* na svim mikrokontrolerima, dok se brže izvršava *ChaCha20* zavisno od veličine ključa i testiranog mikrokontrolera.

TABELA 3 REZULTATI ANALIZE PERFORMANSI BLOK METODA NA *FELICS* PLATFORMI

| Metoda | Parametri metoda | | *AVR* | | | *MSP* | | | *ARM* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Blok [b] | Ključ [b] | Kod [B] | RAM [B] | Vreme [takt] | Kod [B] | RAM [B] | Vreme [takt] | Kod [B] | RAM [B] | Vreme [takt] |
| *SPECK* | 64 | 96 | 956 | 292 | 40666 | 576 | 290 | 36698 | 328 | 304 | 16100 |
| *SPECK* | 64 | 128 | 864 | 300 | 45686 | 592 | 298 | 37850 | 402 | 312 | 17084 |
| *SIMON* | 64 | 96 | 1074 | 361 | 64440 | 758 | 362 | 50932 | 466 | 376 | 24591 |
| *SIMON* | 64 | 128 | 1112 | 373 | 67404 | 780 | 374 | 53112 | 530 | 388 | 23404 |
| *Chaskey* | 128 | 128 | 1318 | 227 | 21349 | 900 | 222 | 19058 | 450 | 236 | 8740 |
| *Chaskey-LTS* | 128 | 128 | 1318 | 227 | 33829 | 904 | 222 | 29170 | 450 | 236 | 11556 |

TABELA 4 REZULTATI ANALIZE PERFORMANSI STRIM METODA NA *FELICS* PLATFORMI

| Metoda | Parametri metoda | | | *AVR* | | | *MSP* | | | *ARM* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Stanje [b] | Ključ [b] | IV [b] | Kod [B] | RAM [B] | Vreme [takt] | Kod [B] | RAM [B] | Vreme [takt] | Kod [B] | RAM [B] | Vreme [takt] |
| *ChaCha20* | 512 | 128 | 64 | 1042 | 313 | 53723 | 744 | 312 | 36999 | 740 | 380 | 7095 |
| *ChaCha20* | 512 | 256 | 64 | 1156 | 328 | 52737 | 768 | 328 | 36987 | 748 | 396 | 7163 |
| *Trivium* | 288 | 80 | 80 | 1130 | 211 | 92985 | 980 | 212 | 70602 | 872 | 300 | 13512 |

### D. Izbor metoda lake kriptografije

Ustanovljeno je da se na *IoT* uređajima mogu koristiti kriptografske metode, uprkos otkrivenim nedostacima, ukoliko postižu prihvatljiv stepen zaštite na uređajima sa ograničenim resursima [22]. Da bi se postigao kompromis između sigurnosti i performansi, kod *IoT* uređaja je potrebno razmotriti veličinu ključa, broj iteracija i složenost operacija. Viši stepen sigurnosti se postiže većim ključevima, većim brojem iteracija i složenijim algoritmima, što istovremeno opterećuje raspoložive registre i memoriju, smanjuje brzinu izvršavanja algoritma i povećava potrošnju energije. U zavisnosti od hardverske ili softverske implementacije, složenost algoritma utiče i na iskorišćenje površine čipa ili veličinu koda koji se smešta u memoriji uređaja. Stoga je potrebno prilagoditi implementaciju kriptografskog algoritma u zavisnosti od funkcije uređaja i njegovih raspoloživih resursa. Izbor metoda zavisi i od potreba uređaja kada su u pitanju odziv i protok, posebno kod aplikacija i uređaja koji moraju da reaguju u realnom vremenu, kao i napajanje uređaja i potrošnja energije, posebno kod uređaja koji imaju ograničen izvor napajanja.

### E. Pregled pravaca daljeg istraživanja

S obzirom na predikcije o porastu broja *IoT* uređaja u bliskoj budućnosti, laka kriptografija je ključna za dalji razvoj tehnologije Interneta stvari i očuvanje privatnosti podataka. Dalji rad u oblasti lake kriptografije podrazumeva praćenje stepena sigurnosti postojećih metoda, analiza performansi na budućim *IoT* uređajima, kao i sticanje znanja i razvijanje novih algoritama na osnovu dosadašnjih iskustva. Visok stepen sigurnosti i dobre performanse su ključne za dizajn i arhitekturu budućih *IoT* sistema.

Problem poređenja performansi kriptografskih metoda zahteva nastavak procesa međunarodne standardizacije i pronalaženje pouzdanog sistema za analizu performansi. U idealnom slučaju, kriptografska zajednica bi se oslanjala na jedinstvenu bazu kriptografskih algoritama, koja bi sadržala sve postojeće implementacije metoda, specifikacije i informacije o stepenu sigurnosti, kao i performansama ovih metoda na različitim uređajima Interneta

stvari. Ovakav sistem bi znatno olakšao dalja istraživanja i širenje znanja u oblasti lake i klasične kriptografije.

## VI. ZAKLJUČAK

Ovaj rad predstavlja pregled stanja u oblasti lake kriptografije, kako u dosadašnjim istraživanjima u svetu, tako i na domaćem nivou. Bavi se analizom metoda lake kriptografije, kao i poređenjem njihovih performansi na uređajima sa ograničenim resursima.

## VII. LITERATURA


[1] *International Telecommunication Union* (2012), *Recommendation ITU-T Y.2060*, "*Overview of the Internet of things*", dostupno na https://handle.itu.int/11.1002/1000/11559 (pristupljeno: februar, 2023)

[2] *Carnegie Mellon University Computer Science Department Coke Machine*, dostupno na https://www.cs.cmu.edu/~coke/history_long.txt (pristupljeno: februar, 2023)

[3] *Cisco* (2020*), "Cisco Annual Internet Report (2018-2023)*", *white paper edition*, *Cisco*, *San Jose*

[4] *IoT Analytics* (2022), "*IoT Analytics Research 2022*", *IoT Analytics*, *Hamburg*, dostupno na https://iot-analytics.com/number-connected-iot-devices/ (pristupljeno: februar, 2023)

[5] *5G Americas* (2019), "*5G Spectrum Vision*", *5G Americas White Paper*, *5G Americas*, *Washington*

[6] *Cisco* (2023), "*What Is 5G vs 4G?*", *Cisco Systems*, *San Jose*, dostupno na https://www.cisco.com/c/en/us/solutions/what-is-5g/5g-vs-4g.html (pristupljeno: februar, 2023)

[7] *Palattella Maria Rita*, *Dohler Mischa*, *Grieco Luigi Alfredo*, *Rizzo Gianluca*, *Torsner Johan*, *Engel Thomas*, *Ladid Latif* (2016), "*Internet of Things in the 5G Era: Enablers, Architecture and Business Models*", *IEEE Journal on Selected Areas in Communications*. 34. 1-1. doi: 10.1109/JSAC.2016.2525418.

[8] *Ericsson* (2018), "*5g security, scenarios and solutions*", *white paper*, *Ericsson*, *Stockholm*

[9] *Telenor IoT* (2023), "*5G and IoT: What can 5G do for IoT business?*", *white paper*, *Telenor IoT*, *Solna*

[10] *Atzori Luigi*, *Iera Antonio*, *Morabito Giacomo* (2010), "*The Internet of Things: A Survey*", *Computer Networks*. 2787-2805. doi: 10.1016/j.comnet.2010.05.010.

[11] *Shafiq Muhammad*, *Gu Zhaoquan*, *Cheikhrouhou Omar*, *Alhakami Wajdi*, *Hamam Habib* (2022), "*The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks*", *Wireless Communications and Mobile Computing*. 2022. 12. doi: 10.1155/2022/8669348.

[12] *McKay Kerry*, *Bassham Larry*, *Turan Meltem Sönmez*, *Mouha Nicky* (2016), "*Report on Lightweight Cryptography*", *NIST Internal Report 8114*, *NIST*, *Gaithersburg*

[13] *NIST* (2017), "*Lightweight Cryptography Project*", *Computer Security Resource Center*, *NIST*, *Gaithersburg*, dostupno na https://csrc.nist.gov/projects/lightweight-cryptography (pristupljeno: februar, 2023)

[14] *ISO* (1989), *ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection*, *International Organization for Standardization*, *Geneva*, dostupno na https://www.iso.org/committee/45306.html (pristupljeno: februar, 2023)

[15] *ISO* (2012), *ISO/IEC 29192 Information technology - Security techniques - Lightweight cryptography*, *International Organization for Standardization*, *Geneva*, dostupno na https://www.iso.org/standard/56425.html (pristupljeno: februar, 2023)
[16] *ISS* (2018), *SRPS ISO/IEC 29192-2:2018* Informacione tehnologije - Tehnike bezbednosti - Laka kriptografija, Institut za standardizaciju Srbije, Beograd, dostupno na https://iss.rs/sr_Cyrl/project/show/iss:proj:65370 (pristupljeno: februar, 2023)
[17] *ISS* (2018), *SRPS ISO/IEC 29192-2:2020* Informacione tehnologije - Laka kriptografija, Institut za standardizaciju Srbije, Beograd, dostupno na https://iss.rs/sr_Cyrl/project/show/iss:proj:74073 (pristupljeno: februar, 2023)
[18] *ISO* (2018), *ISO/IEC 29167-21:2018 Information technology - Automatic identification and data capture techniques*, *International Organization for Standardization*, *Geneva*, dostupno na https://www.iso.org/standard/70388.html (pristupljeno: februar, 2023)
[19] *ISO* (2018*), ISO/IEC 29167-22:2018 Information technology - Automatic identification and data capture techniques*, *International Organization for Standardization*, *Geneva*, dostupno na https://www.iso.org/standard/70389.html (pristupljeno: februar, 2023)
[20] *ETSI* (2020), "*Cyber Security for Consumer Internet of Things: Baseline Requirements*", *European Telecommunications Standards Institute, Sophia Antipolis*
[21] *Okamura Toshihiko* (2017), "*Lightweight Cryptography Applicable to Various IoT Devices*", *NEC Technical Journal*. Vol.12. No.1
[22] *Mouha Nicky* (2015), "*The Design Space of Lightweight Cryptography*", *IACR Cryptol. ePrint Arch.* 2015 (2015): 303.
[23] *Buchanan William, Li Shancang, Asif Rameez* (2017), "*Lightweight cryptography methods*", *Journal of Cyber Security Technology*, 1:3-4, 187-201, doi: 10.1080/23742917.2017.1384917
[24] *Feizi Soheil, Ahmadi Arash, Nemati Ali* (2014), "*A hardware implementation of Simon cryptography algorithm*". *4th International Conference on Computer and Knowledge Engineering, ICCKE* 2014. 245-250. doi: 10.1109/ICCKE.2014.6993386.
[25] *Beaulieu Ray, Shors Douglas, Smith Jason, Treatman-Clark Stefan, Weeks Bryan, Wingers Louis* (2013), "*The SIMON and SPECK Families of Lightweight Block Ciphers*", *Cryptology ePrint Archive, Paper* 2013/404, dostupno na https://eprint.iacr.org/2013/404 (pristupljeno: februar, 2023)
[26] *Shannon Claude* (1949), "*Communication theory of secrecy systems*", *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, doi: 10.1002/j.1538-7305.1949.tb00928.x.
[27] *Bernstein, Daniel* (2008), "*The Salsa20 Family of Stream Ciphers*", *The eSTREAM Finalists*, doi: 10.1007/978-3-540-68351-3_8
[28] *Bernstein, Daniel* (2008), "*ChaCha, a variant of Salsa20*", dostupno na https://cr.yp.to/chacha/chacha-20080128.pdf (pristupljeno: februar, 2023)
[29] *De Cannière Christophe, Preneel Bart* (2008), "*TRIVIUM*", *The eSTREAM Finalists*, doi: 10.1007/978-3-540-68351-3_8
[30] *eSTREAM* 2004-2008, *ECRYPT Stream Cipher Project*, dostupno na https://www.ecrypt.eu.org/stream/ (pristupljeno: februar, 2023)
[31] *Potestad-Ordóñez Francisco, Valencia-Barrero Manuel, Baena-Oliva Carmen, Parra-Fernández Pilar, Jiménez-Fernández Carlos* (2020), "*Breaking Trivium Stream Cipher Implemented in ASIC Using Experimental Attacks and DFA*", Sensors. 20. 6909. doi: 10.3390/s20236909.
[32] *Guo Jian, Peyrin Thomas, Poschmann Axel* (2011), "*The PHOTON Family of Lightweight Hash Functions*", *31st Annual Cryptology Conference, International Association for Cryptologic Research, Santa Barbara*
[33] *Bogdanov Andrey, Knezevic Miroslav, Leander Gregor, Toz Deniz, Varici Kerem, Verbauwhede Ingrid* (2013) "*SPONGENT: The Design Space of Lightweight*

*Cryptographic Hashing*", *IEEE Transactions on Computers*, vol. 62, no. 10, pp. 2041-2053. doi: 10.1109/TC.2012.196.
[34] *Mouha Nicky, Mennink Bart, Van Herrewege Anthony, Watanabe Dai, Preneel Bart, Verbauwhede Ingrid* (2014), "*Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers*", *ACM Symposium on Applied Computing*, doi: 10.1007/978-3-319-13051-4_19
[35] *Dinu Daniel, Biryukov Alex, Großschädl Johann, Khovratovich Dmitry, Le Corre Yann, Perrin Léo* (2015), "*FELICS - Fair Evaluation of Lightweight Cryptographic Systems*", *University of Luxembourg*
[36] *CryptoLUX, FELICS, Departement of Computer Science, University of Luxembourg*, dostupno na https://www.cryptolux.org/index.php/FELICS (pristupljeno: februar, 2023)
[37] *Yu Jenny, Aagaard Mark* (2019), "*Benchmarking and Optimizing AES for Lightweight Cryptography on ASICs*"
[38] Prvulović Petar, Radosavljević Nemanja, Babić Đorđe (2021), "Pregled "lakih" blok-šifarskih algoritama zasnovanih na SPN mreži sa aspekta bezbednosti bežičnih senzorskih mreža", *20th International Symposium INFOTEH-JAHORINA, conference paper*
[39] Prvulović Petar, Radosavljević Nemanja, Babić Đorđe (2021), "*Analysis of Lightweight Cryptographic Protocols in Precision Agriculture - A Case Study*", *15th International Conference on Advanced Technologies, Systems and Services in Telecommunications* (*TELSIKS*), Niš, pp. 295-298, doi: 10.1109/TELSIKS52058.2021.9606294.

## ABSTRACT

The latest reports and Internet statistics predict that the number of devices connected to IP networks will be more than three times larger than the global population by the end of 2022. The increase in the number of devices is closely related to advancements in industry and the development of mobile communication systems, as well as the enormous increase of mobile users, followed by the development of 5G networks and Internet of Things (IoT). However, with technological advancements in IoT, devices that do not have enough resources for execution of complex algorythms but still require certain level of security, become more common. Lightweight Cryptography is a technology that aims to provide secure communication to such devices, taking into account their limited power, processing, and memory resources. Lightweight cryptography by definition is a cryptographic algorithm or protocol designed for use in restricted environments, which extends the use of cryptography to devices with limited resources (including *RFID* tags, sensors, contactless smart cards, medical, and similar devices). International standardization and guidelines for further development in this field are currently underway.

The aim of this master's thesis is twofold. On the one hand, the thesis presents theoretical concepts, algorithms, and protocols related to the implementation of security protocols in the Internet of Things. An overview of proposed standards is provided, including *ISO/IEC JTC 1/SC 27* group and *ISO/IEC 29192* standard, the latest standardization project. The hardware and software characteristics of systems that condition the implementation of lightweight cryptography, such as chip architecture, RAM size, algorithm implementation size, and energy consumption, are also discussed. On the other hand, the thesis presents several different lightweight cryptography methods, which include different approaches and have attracted the most attention from

the professional community. The operation and application of each method are explained. Then, the required resources and performance of the methods are analyzed, using different microcontrollers that simulate the operation of microprocessors in the Internet of Things technology. The results are presented and compared in tables. Finally, the drawbacks and potential attacks on these methods are discussed, as well as the future application and further development of lightweight cryptography within the Internet of Things technology.

*Key words* – Internet of Things, 5G IoT, Lightweight cryptography, Lightweight cryptography methods, Block ciphers, Stream ciphers, Hash functions, Digital signature, *SIMON*, *SPECK*, *CHACHA*, *TRIVIUM*, *PHOTON*, *SPONGENT*, *CHASKEY*, *FELICS*

**ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHY METHODS**

Nataša Dimić, Mirjana Radivojević