ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Մինասյան Համբարձում Դավթի

ԻՐԵՐԻ ՀԱՄԱՑԱՆՑԻ ՍԱՐՔԱՎՈՐՈՒՄՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՄԵԹՈԴՆԵՐԻ և ԳՈՐԾԻՔԱՄԻՋՈՑՆԵՐԻ ՄՇԱԿՈՒՄԸ

Ե.13.04 – «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի
գիտական աստիճանի հայցման ատենախոսության

Ս Ե Ղ Մ Ա Գ Ի Ր

Երևան – 2026

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ НАН РА

Минасян Амбарцум Давидович

РАЗРАБОТКА МЕТОДОВ И ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.04 «Математическое и программное обеспечение вычислительных машин, комплексов, систем и сетей»

Ереван – 2026

Ատենախոսության թեման հաստատվել է Հայաստանի ազգային պոլիտեխնիկական համալսարանում:

Գիտական ղեկավար՝	տեխ.գիտ.թեկնածու, պրոֆ.	Գ.Ի.Մարգարով
Պաշտոնական ընդդիմախոսներ՝	տեխ.գիտ.դոկտոր	Ս.Ս.Սարգսյան
	տեխ.գիտ.թեկնածու	Թ.Վ.Ջամղարյան
Առաջատար կազմակերպություն՝	Երևանի կապի միջոցների գիտահետազոտական ինստիտուտ	

Պաշտպանությունը կայանալու է 2026թ. Հունիսի 2-ին, ժ.12:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:
Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ գրադարանում:
Սեղմագիրը առաքված է 2026թ. ապրիլի 30-ին:

037 Մասնագիտական խորհրդի
գիտական քարտուղար ֆ.մ.գ.դ. պրոֆ. Մ.Ե.Հարությունյան

Тема диссертации утверждена в Национальном политехническом университете Армении.

Научный руководитель:	кандидат тех. наук, проф.	Г.И. Маргаров
Официальные оппоненты:	доктор тех. наук,	С.С. Саргсян
	кандидат тех. наук	Т.В.Джамгарян
Ведущая организация:	Ереванский научно-исследовательский институт связи	

Защита состоится 2-ого июня 2026г. в 12:00 на заседании специализированного совета 037 «Информатика» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.
С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.
Автореферат разослан 30-ого апреля 2026г.

Ученый секретарь,
Специализированного совета 037
доктор физ.-мат.наук, профессор. М.Е.Арутюнян

ԱՇԽԱՏԱՆՔԻ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Աշխատանքի արդիականությունը: Իրերի համացանցի (Internet of Things - IoT) սարքերի մեծ տեմպերով զարգացումը և դրանց կիրառման ոլորտների ընդլայնումը հանգեցրել են կիբեռանվտանգության նոր մարտահրավերների առաջացմանը: IoT էկոհամակարգը թիրախավորող ժամանակակից կիբեռհարձակումները դարձել են բազմաշերտ և բարդ, մինչդեռ ներկայումս կիրառվող սարքերի զգալի մասը կա՛մ չունի ներկառուցված անվտանգության մեխանիզմներ, կա՛մ հիմնվում է կենտրոնացված ամպային լուծումների վրա. այն պահանջում է մշտական կապ, ինչը անիրագործելի է իրական կիրառությունների մեծ մասի դեպքում: IoT սարքերին բնորոշ ռեսուրսների սահմանափակումները՝ հաշվողական հզորության, հիշողության և էներգիայի սպառման տեսանկյուններից, էլ ավելի են բարդացնում անվտանգության ավանդական մոտեցումների կիրառումը: Առկա է հիմնարար հակասություն տեղեկատվության պաշտպանության խիստ պահանջների և IoT ապարատային ապահովման սահմանափակ հնարավորությունների միջև: Թեև ժամանակակից բջջային IoT պլատֆորմները (օրինակ՝ Nordic nRF9161) ինտեգրում են ապարատային անվտանգության մոդուլներ (ARM CryptoCell-310, TrustZone), սակայն բացակայում են դրանց արդյունավետ օգտագործման համակարգված մեթոդները՝ սարքի կիրառման ամբողջական կենսացիկլի գործունեության համար: Միևնույն ժամանակ, RFC 9783 ստանդարտի (PSA ատեստավորման տոկեն) վերջին հրապարակումը ստեղծում է հնարավորություն՝ սարքերի կարգավիճակի գնահատման համար, սակայն դրա կիրառելիությունը սահմանափակ ռեսուրսներով սարքերի վրա դեռևս գործնականում հաստատված չէ: Վերոնշյալ խնդիրների լուծմանն ուղղված մեթոդների և գործիքների մշակման անհրաժեշտությունն է սույն ատենախոսական աշխատանքի արդիականության հիմնավորումը:

Այսպիսով, իրերի համացանցի սարքավորումների համար նախատեսված գաղտնագրման համակարգերի մշակման խնդիրն արդիական է թե՛ գիտական հետաքրքրություն ներկայացնող խնդիրների լուծման, և թե՛ կիրառական նշանակություն ունեցող ավտոմատացված կառավարում պահանջող համակարգերի նախագծման տեսանկյունից:

Աշխատանքի նպատակն է մշակել մեթոդներ և գործիքներ՝ իրերի համացանցի սարքերի անվտանգության ապահովման համար: Նշված նպատակին հասնելու համար աշխատանքում դրվել և լուծվել են հետևյալ խնդիրները.

- Մշակել իրերի համացանցի սարքավորումների գաղտնակայունության գնահատման մաթեմատիկական մոդել.
- Մշակել գաղտնագրման բանալիների գեներացման, պահպանման և փոխանակման ապահովման մեթոդներ.
- Մշակել իրական ժամանակում իրերի համացանցի սարքավորումների կարգավիճակի և անվտանգության մակարդակի գնահատման մեթոդ:

Գիտական արդյունքները:

- Մշակվել է գաղտնագրման համակարգի արդյունավետության գնահատման մաթեմատիկական մոդել, որն ի տարբերություն առկա լուծումների՝ ինտեգրում է էներգասպառումը, հաշվարկային ցիկլերը և հիշողության սահմանափակումները:

- Առաջարկվել են իրերի համացանցի սարքավորումների գաղտնագրման համար օգտագործվող բանալիների գեներացման, պահպանման և փոխանակման մեթոդներ, որոնք, ի տարբերություն առկա լուծումների, չեն պահանջում կենտրոնացված համակարգեր և հիմնված են ապարատային լուծման վրա:

- Առաջարկվել է իրերի համացանցի սարքավորումների վիճակի և անվտանգության մակարդակի գնահատման մեթոդ, որն ի տարբերություն առկա լուծումների՝ կատարում է սարքավորման վարքագծի իրական ժամանակում վերլուծություն և հնարավորություն է տալիս՝ կատարելու հեռահար մշտադիտարկում:

Աշխատանքի կիրառական նշանակությունը: Մշակված լուծումները կիրառելի են խելացի տների, արդյունաբերության ավտոմատացման, առողջապահության և խելացի քաղաքների ենթակառուցվածքներում: Ապարատային արագացմամբ բանալիների կառավարման մեթոդը զգալիորեն երկարացնում է մարտկոցով աշխատող սարքերի կենսունակությունը, ինչը տնտեսապես արդյունավետ է դժվար հասանելի վայրերում տեղակայված տվիչների դեպքում: Մշակված համագործակցային ճարտարապետության կիրառության միջոցով բանալիների կառավարումն ապահովում է մասշտաբայնություն տասնյակ հազարավոր սարքերի համար:

Արդյունքների ներդրումը: Ատենախոսության շրջանակներում մշակված բանալիների կառավարման և սարքերի կարգավիճակի գնահատման համակարգերը ներդրվել են «Ար Փի Ի Քնթրոլս» ՍՊԸ-ում (RPE Controls LLC)՝ խելացի կառավարվող լուծումների անվտանգության մակարդակի բարձրացման նպատակով: Գաղտնագրման գործընթացի կայունության գնահատման մաթեմատիկական մոդելը և դրա ծրագրային իրականացումն օգտագործվում են Հայաստանի ազգային պոլիտեխնիկական համալսարանի «Տեղեկատվական անվտանգության և ծրագրային ապահովման» ամբիոնի ուսումնական գործընթացում:

Հրապարակումներ: Ատենախոսության հիմնական արդյունքները տպագրված են 7 գիտական աշխատանքներում և հեղինակային իրավունքների պաշտպանության 1 արտոնագրով, որոնք թվարկված են սեղմագրի վերջում:

Աշխատանքի կառուցվածքը և ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, չորս գլխից, եզրակացությունից, օգտագործված գրականության ցանկից և հավելվածներից: Աշխատանքի ընդհանուր ծավալը կազմում է 130 էջ:

ԱՇԽԱՏԱՆՔԻ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածություն: Ներածության մեջ հիմնավորված է թեմայի արդիականությունը, ձևակերպված են աշխատանքի նպատակները, գիտական նորույթները և հիմնական դրույթները, որոնք ներկայացվում են պաշտպանության:

Գլուխ 1-ում ներկայացվում է ատենախոսությունում կիրառված տեխնոլոգիաների և մոտեցումների նկարագրությունը: Վերլուծությունը ցույց է տվել, որ սպառնալիքների միջավայրը կտրուկ սրվել է՝ IoT վերջնակետային սարքերի վրա օրական մոտ 820,000 հարձակումներով և խախտման փորձերի տարեկան 84% աճով: Աշխատանքի այս հատվածում ներկայացվել է առկա հետազոտություններում հինգ կարևոր բացթողում. բանալիների կառավարման համապարփակ՝ ապարատային արագացմամբ շրջանակների բացակայությունը, բանալիների կառավարման նախագծման մեջ էներգիա-անվտանգություն փոխզիջումներին ոչ բավարար ուշադրությունը, մառախլապատ (fog-assisted) անվտանգության ճարտարապետությունների սահմանափակ մասշտաբայնությունը, IoT սահմանափակումներին հարմարեցված սարքերի ստանդարտացված հավաստագրման բացակայությունը և գաղտնիությունը պահպանող ու քվանտային կայուն մեխանիզմների ոչ բավարար ինտեգրումը:

Գլուխ 2-ում ներկայացվել են սահմանափակ ռեսուրսներով IoT սարքերի վրա ապարատային գաղտնագրման համակարգերի մոդելավորման և քանակական գնահատման համար մաթեմատիկական մոդելներ: Ներկայացված համակարգը հնարավորություն է տալիս կազմել էներգիայի սպառման, անվտանգության մակարդակի, հիշողության օգտագործման և հաշվողական ծախսերի միջև կապերը՝ օպտիմալացման մոդելի միջոցով, որը ենթարկվում է անվտանգության և ռեսուրսների հստակ սահմանափակումների:

Սահմանափակ ռեսուրսներով սարքերում գաղտնագրման գործողությամբ սպառվող էներգիան բաղկացած է դինամիկ և ստատիկ բաղադրիչներից: Մոդելավորվել է ընդհանուր էներգիան՝ E.

$$E = E_{dyn} + E_{stat} = \alpha \cdot V^2 \cdot C_{sw} \cdot f \cdot N + \beta \cdot I_{leak} \cdot t_{op}$$

Որտեղ α-ն՝ դինամիկ հզորության մասշտաբավորման գործակիցն է (կախված է տեխնոլոգիայից, սովորաբար 0.8–1.0 է), V-ն՝ սնուցման լարումը (Վ), C_{sw}-ն՝ արդյունավետ փոխարկվող տարողությունը (Ֆ),f-ը՝ տակտային հաճախականությունը (Հց),N-ը՝ գործողության համար անհրաժեշտ տակտային ցիկլերի թիվը,β-ն՝ արտահոսքի մասշտաբավորման գործակիցը, I_{leak}-ը՝ արտահոսքի հոսանքը (Ա), $t_{op} = N/f$-ը գործողության տևողությունը (վ):

Առաջարկվում է կիրառել գաղտնագրային արդյունավետության միասնական ինդեքս (Unified Cryptographic Efficiency Index - UCEI), որն ինտեգրում է ռեսուրսների բոլոր չափումները մեկ համադրելի սկալյար արժեքի մեջ: Սա ընդլայնում է նախկինում հրապարակած արժեքի ֆունկցիան $\phi(E,T,M)$՝ վերածելով այն նորմալացված, կշռված բաղադրյալ չափորոշիչի:

P պլատֆորմի վրա աշխատող A ալգորիթմի դեպքում գաղտնագրային արդյունավետության միասնական ինդեքսը սահմանվում է որպես.

$$\mathrm{UCEI}(A,P) = \left(\frac{\Theta_A}{\Theta_{ref}}\right)^{w_1} \cdot \left(\frac{E_{ref}}{E_A}\right)^{w_2} \cdot \left(\frac{M_{ref}}{M_A}\right)^{w_3} \cdot \left(\frac{S_A}{S_{ref}}\right)^{w_4}$$

որտեղ Θ_A, E_A, M_A, S_A – և ալգորիթմի թողունակությունը, էներգիան, հիշողությունը և անվտանգության մակարդակներն են, $\Theta_{ref}, E_{ref}, M_{ref}, S_{ref}$-ը՝ ելակետային (reference) արժեքները (ստանդարտ AES-128, ECC-256, SHA-256), w_1, w_2, w_3, w_4-ը կշռային գործակիցները, որոնք բավարարում են $w_1 + w_2 + w_3 + w_4 = 1$ պայմանին:

UCEI արժեքը չափողականություն չունի. 1.0-ից մեծ արժեքները ցույց են տալիս բարելավում ելակետային իրականացման նկատմամբ, իսկ 1.0-ից փոքր արժեքները՝ վատթարացում: Ներկայացված մոտեցում աշխատանքի հրապարակման պահին առաջարկ է կատարվել առաջին անգամ, նմանատիպ գնահատման այլ մեթոդները չեն ներառում ներկայացված գնահատման 4 պարամետրերը:

Առաջարկվել են երեք օպտիմալացված թեթևագույն (lightweight) գաղտնագրման ալգորիթմներ՝ AES-128-L (AES-ի թեթև տարբերակ), ECC-163 (օպտիմալացված էլիպսաձև կորի իրականացում) և BLAKE2s-HW (ապարատային արագացմամբ հեշ ֆունկցիա): Փորձարարական գնահատումը չորս IoT հարթակներում (VisionFive 2, Nordic nRF9161, ESP32-S3, Arduino Uno) ցույց է տվել էներգիայի սպառման՝ միջինը 47% կրճատում, հիշողության օգտագործման 62% նվազում և թողունակության 35% բարելավում ստանդարտ իրականացումների համեմատ՝ պահպանելով 128-բիթանոց բանալիների կիրառության անվտանգության մակարդակը:

Կիրառելով UCEI բանաձևը մարտկոցով սնուցվող տվիչի պրոֆիլով ($w_1 = 0.15, w_2 = 0.40, w_3 = 0.30, w_4 = 0.15$) և օգտագործելով nRF9161-ի վրա որպես ելակետ ստացվում են հետևյալ արդյունքները.

Աղյուսակ 1. UCEI արդյունքների համեմատությունը

Ալգորիթմ	**UCEI (Մարտկոցով տվիչ)**	**UCEI (Եզրային երթուղիչ)**	**UCEI (Արդյունաբերական)**
AES-128 (ref)	1.000	1.000	1.000
AES-128-L	2.847	2.312	2.156
BLAKE2s-HW	2.634	2.198	2.043
ECC-163	1.428*	1.195*	0.876*
Ascon-AEAD128	1.682	1.534	1.489
SPECK-128/128	2.124	1.876	1.745

*ECC-163-ը ապահովում է 80-բիթանոց բանալու երկարությանը համարժեք անվտանգություն՝ ի տարբերություն 128-բիթանոցի, ինչը խանգարում է բարձր անվտանգության կշիռ ունեցող պրոֆիլներում:

Coq և Isabelle/HOL թեորեմների ապացուցումների օգտագործմամբ տեսական վավերացումը հաստատել է գաղտնագրման-վերծանման գործողությունների ճշտությունը: Ստորև բերված աղյուսակը ներկայացնում է Պարետո վերլուծության համար օգտագործված տվյալները՝ փորձնական և համեմատական արժեքներով.

Աղյուսակ 2. Գաղտնագրման ալգորիթմների համեմատությունը

Ալգորիթմ	**Պլատֆորմ**	**Էներգիա (մկՋ /գործ.)**	**Հիշող. (ԿԲ)**	**Բանալու երկ. (բիթ)**	**Պարետո-օպտիմա՞լ**
AES-128	nRF9161	42.5	8.2	128	Ոչ
AES-128-L	nRF9161	22.4	3.1	128	**Այո**
AES-128-L	ESP32-S3	18.6	3.1	128	**Այո**
AES-128-L	VisionFive 2	14.2	3.1	128	**Այո**
ECC-256	nRF9161	156.8	12.5	128	Ոչ
ECC-163	nRF9161	68.2	4.8	80	**Այո**
SHA-256	nRF9161	38.6	6.4	128	Ոչ
BLAKE2s-HW	nRF9161	23.1	2.4	128	**Այո**
PRESENT-80	ATmega328P	15.3	1.8	80	**Այո**

Կողմնակի ալիքների վերլուծությամբ (side-channel analysis) հաստատվել է, որ ապարատային լուծումների կիրառմամաբ նվազեցվել են հզորության վերլուծության կոռելյացիայի գործակիցը մինչև 0.03, իսկ անսարքությունների ներարկման պաշտպանությունն ապահովել է մեկ բիթանոց անսարքությունների 99.7% հայտնաբերում:

Առաջարկվում է անվտանգության բաղադրյալ չափորոշիչ (Composite Security Metric -CSM), որն ինտեգրում է դասական անվտանգության մակարդակը, հետքվանտային դիմացկունությունը և կողմնակի ալիքների կայունությունը մեկ գնահատման միավորի մեջ.

A ալգորիթմի համար.

$$\mathrm{CSM}(A) = \min\left(S_{classical}(A),\quad \lambda \cdot S_{pq}(A),\quad \mu \cdot S_{sc}(A)\right),$$

որտեղ $S_{classical}$-ը դասական անվտանգության մակարդակն է բիթերով, S_{pq}-ն՝ հետքվանտային անվտանգության մակարդակն է բիթերով, S_{sc}-ն՝ կողմնակի ալիքների անվտանգության մակարդակ (սահմանված որպես բանալու կորզման համար անհրաժեշտ հետքերի քանակի log_2),λ-ն՝ քվանտային համապատասխանության գործակից (0՝ քվանտային սպառնալիքի բացակայության դեպքում, 1՝ անմիջական քվանտային սպառնալիքի դեպքում), μ-ն՝ ֆիզիկական հասանելիության գործակից (0՝ ֆիզիկական հասանելիության բացակայության դեպքում, 1՝ լրիվ ֆիզիկական հասանելիության դեպքում):

Ժամանակակակից սպառնալիքների պայմաններում ($\lambda \approx 0.1, \mu$-ն փոփոխվում է ըստ տեղակայման) բոլոր առաջարկվող ալգորիթմներն ապահովում են համարժեք անվտանգություն:

Աղյուսակ 3. CSM գնահատումը առաջարկվող ալգորիթմների դեպքում

Ալգորիթմ	S_classical	S_pq	S_sc (HW)	CSM (λ=0, μ=0)	CSM (λ=0.5, μ=0.5)	CSM (λ=1, μ=1)
AES-128-L	128	64	23.3*	128	64	23.3
ECC-163	80	0	22.3*	80	0	0
BLAKE2s-HW	128	85	23.0*	128	85	23.0

**S_sc արժեքները ապարատային իրականացումների վրա բանալու կորզման համար պահանջվող չափված հետքերի $\log_2$-ն են*

Գլուխ 3-ում ներկայացվել է երեք փոխկապակցված մեթոդ, որոնք միասին լուծում են լայնածավալ բջջային IoT տեղակայումների բանալիների կառավարման և տվյալների անվտանգության ապահովման պահանջները:

Առաջինը՝ կիրառվել է համագործակցային բազմակլաստերային մառախլապատ (fog) ճարտարապետություն՝ DANE/DANCE արձանագրություններով բանալիների մասշտաբային կառավարման համար, որն ունի քառաստիճան հիերարխիկ կառուցվածք: Փորձարարական գնահատումը ցույց է տվել մասշտաբայնության 5 անգամ բարելավում (աջակցելով ավելի քան 50,000 սարքերի), հարցումների հաջողության 99.8% մակարդակ:

Երկրորդ՝ մշակվել է բանալիների կառավարման ապարատային արագացմամբ շրջանակ՝ օգտագործելով ARM CryptoCell-310 և TrustZone տեխնոլոգիաները, որն ապահովում է բանալիների անվտանգ գեներացում ապարատային էնտրոպիայի աղբյուրների միջոցով և մեկուսացված պահպանում:

Երրորդ՝ մշակվել է «Խմբաքանակը որպես ծառայություն» (Batch-as-a-Service - BaaS) համակարգ՝ խելացի քաղաքների IoT տեղակայումների համար, որն ինտեգրում է UDP-ից TCP արձանագրության փոխարկումը, դիֆերենցիալ գաղտնիության մեխանիզմները և հետքվանտային հաղորդակցման արձանագրությունները (CRYSTALS-Kyber, CRYSTALS-Dilithium):

Թվային տվիչներից տեղեկատվության հավաքագրման համար (երթևեկության հաշվարկներ, միջին արագություններ, ջերմաստիճանի ընթերցումներ) կիրառվում է Լապլասի մեխանիզմը: Համաձայն Սինթիա Դվորկի «Դիֆերենցված գաղտնիություն» 2006 հրապարակված հոդվածի՝ տրված $f:\mathcal{D}\to\mathbb{R}^{\mathbb{k}}$ հարցման ֆունկցիայի համար $\Delta f = \max_{D,D'} |f(D)-f(D')|_1$ զգայունությամբ մեխանիզմն ավելացնում է հավասարակշռված աղմուկ.

$$\mathcal{M}(D) = f(D) + \text{Lap}\left(\frac{\Delta f}{\varepsilon}\right)^k,$$

որտեղ $\text{Lap}(\lambda)^k$-ը նշանակում է k անկախ ընտրություններ Լապլասի բաշխումից $\lambda = \Delta f / \varepsilon$ մասշտաբի պարամետրով:

Սահմանվում է $\varepsilon = 1.0$՝ հիմնվելով խելացի քաղաքների երթևեկության կառավարման տվյալների համար օգտակարություն-գաղտնիություն փոխզիջման համակարգային վերլուծության վրա:

Խելացի քաղաքների IoT տեղակայումները գեներացնում են տվյալների հսկայական ծավալներ տարասեռ սենսորային ցանցերից՝ երթևեկության մոնիտորներ, շրջակա միջավայրի սենսորներ, կոմունալ հաշվիչներ և հսկողության համակարգեր՝ ստեղծելով հիմնարար լարվածություն գործառական արդյունավետության և քաղաքացիների գաղտնիության միջև: IoT սարքերի մեծ մասը հաղորդակցվում է UDP-ով՝ իր ցածր ծախսի շնորհիվ, մինչդեռ ամպային վերլուծական հարթակները պահանջում են TCP հուսալիություն:

BaaS համակարգն ապահովել է ամպային թրաֆիկի 73% կրճատում և սարքերի էներգախնայողության 38% բարելավում:

Անցումային ժամանակաշրջանում (երբ քվանտային համակարգիչներ կարող են գոյություն ունենալ, բայց դասական վստահության արմատները դեռ առկա են) անվտանգությունն ապահովելու համար BaaS-ը կիրառում է հիբրիդային բանալու ձևավորում՝ համատեղելով դասական և հետքվանտային բաղադրիչները.

$$K_{\text{session}} = \text{KDF}(K_{\text{classical}} | K_{\text{PQ}}),$$

որտեղ $K_{\text{classical}}$-ը դուրս է բերվում ECDH-ից (X25519) և K_{PQ}-ն դուրս է բերվում ML-KEM-ից (Kyber-768): Այս հիբրիդային մոտեցումը երաշխավորում է, որ նստաշրջանի բանալին մնա անվտանգ այնքան ժամանակ, քանի դեռ կամ դասական, կամ հետքվանտային բաղադրիչը մնում է չկոտրված ապահովելով պաշտպանություն տեղեկատվության գաղտնագրման ընթացքում: Հիբրիդային մոտեցումն արտացոլում է այն տեղակայման ռազմավարությունները, որոնք արդեն ընդունվել են Chrome-ի, Signal-ի և iMessage-ի կողմից: Մոտեցումը նախագծելիս հաշվի է առնվել Աբդուլ Ահադ Ֆոլի կողմից կատարված հետազոտությունը, ինչը հրապարակվել է հետքվանտային գաղտնագրման վերաբերյալ գիտական հոդվածով(2025):

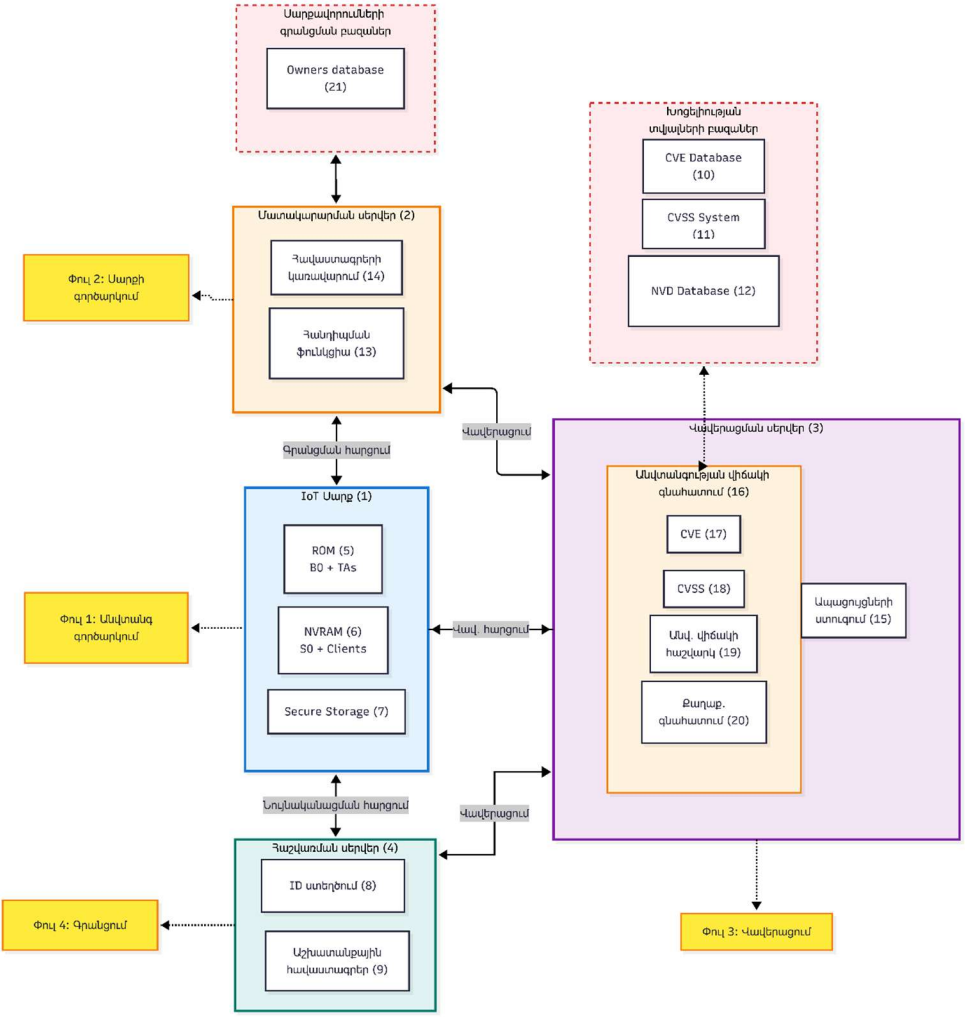
Ատենախոսության երեք գլուխները կազմում են փոխկապակցված հետազոտական շրջանակ, որտեղ յուրաքանչյուր գլուխ հիմնվում է նախորդի արդյունքների վրա և ընդլայնում դրանք: Գլուխ 2-ում մշակված մաթեմատիկական մոդելները, մասնավորապես UCEI և CSM չափորոշիչները, ծառայել են որպես քանակական հիմք Գլուխ 3-ի ապարատային արագացմամբ բանալիների կառավարման շրջանակի նախագծման համար: Էներգիայի սպառման մոդելը թույլ է տվել օպտիմալացնել ARM CryptoCell-310-ի կիրառման պարամետրերը: CSM չափորոշիչի կողմից սահմանված անվտանգության պահանջները իրենց հերթին կողմնորոշել են BaaS համակարգում հիբրիդային բանալու ձևավորման ընտրությունը՝ ապահովելով պաշտպանություն ինչպես դասական, այնպես էլ քվանտային սպառնալիքների դեմ: Դիֆերենցիալ գաղտնիության մեխանիզմների ինտեգրումը մառախլապատ ճարտարապետության հետ ամբողջացնում է անվտանգության բազմաշերտ մոտեցումը՝ ստեղծելով համակարգ, որտեղ մաթեմատիկական երաշխիքները, ապարատային վստահության արմատները և մասշտաբային ճարտարապետությունը գործում են որպես միասնական ամբողջություն:

Այնուամենայնիվ, բանալիների կառավարման և տվյալների պաշտպանության ապահովումը կազմում է IoT սարքերի անվտանգության ապահովման միայն մի մասը:

Հավասարապես կարևոր է սարքի ստուգելի, անվտանգ և վստահելի վիճակի հավաստիացման հարցը: Հենց այս խնդրի լուծմանն է նվիրված գլուխ 4-ը:

Գլուխ 4-ում ներկայացվել է մշակված գործիքների և առաջարկվող մեթոդների համապարփակ փորձարարական վավերացում: ARM TF-M-ի (Trusted Firmware-M) վրա կիրառվել է RFC 9783 PSA հավաստագրման թոքենների համակարգը՝ ապահովելով իրական ժամանակում սարքի կարգավիճակի մշտադիտարկում: Սարքի վիճակի գնահատման ընդհանուր ճարտարապետությունը ներկայացված է բլոկ-դիագրամով.

Նկ. 1. IoT սարքի անվտանգության վիճակի գնահատման համակարգի բլոկ-սխեմա



ARM Cortex-M երեք հարթակների (M33, M4, M0+) վրա փորձարկումները ցույց տվեցին, որ PSA թոքենի գեներացումը պահանջում է միջինը 23.4 մվ Cortex-M33-ի վրա ECDSA ալգորիթմի կիրառմամբ տեղեկատվության պաշտպանության ապահովման համար:

Աղյուսակ 4. PSA Ատեստավորման թոքենի արդյունավետության չափումները

Պլատֆորմ	**Գեներացման տևողությունը (մվ)**	**Ստուգման տևողությունը (մվ)**	**Peak RAM (ԿԲ)**	**Թոքենի չափ (բայթ)**
Cortex-M33 (ECDSA)	23.4	18.7	4.2	380
Cortex-M33 (HMAC)	8.2	6.1	3.1	320
Cortex-M4	31.8	25.2	4.0	380
Cortex-M0+	68.4	54.1	3.8	380

Գործիքն իրականացնում է իրական ժամանակի անոմալիաների հայտնաբերման գործառույթ՝ հիմնված անվտանգության վիճակի ելակետային չափումներից շեղումների վրա: Յուրաքանչյուր d սարքի համար պահպանվում է P_d սահող ելակետային վիճակը, որը հաշվարկվում է W ատեստավորման ցիկլերի ընթացքում.

$$\overline{P_d} = \frac{1}{W} \sum_{t=t_0}^{t_0+W-1} P_d(t):$$

Անոմալիայի ահազանգը գործարկվում է, երբ.

$$|P_d(t) - \overline{P_d}| > \tau \,.\, \sigma_d$$

որտեղ σ_d-ն վիճակի միավորների ստանդարտ շեղումն է ելակետային պատուհանի ընթացքում, իսկ τ-ն՝ կարգավորելի զգայունության շեմը (լռելյայն $\tau = 3$, որը համապատասխանում է 99.7% վստահության միջակայքին նորմալ բաշխման ենթադրությունների ներքո):

Թոքենների քեշավորման օպտիմալացմամբ կրճատվում է ատեստավորման միջին հապաղումը 31%-ով: ProVerif-ով տեսական վավերացումը ներկայացնում է կայուն պաշտպանություն թոքենների կեղծման և վերարտադրման հարձակումներից: Ապարատային արագացմամբ և միայն ծրագրային իրականացումների համեմատական գնահատումը ցույց է տվել 87% բարելավում գաղտնագրման գործողությունների արագության մեջ և 42% կրճատում՝ գաղտնագրային գործողությունների էներգիայի սպառման մեջ: Տնտեսական վերլուծությամբ հաստատվել է, որ սարքի ինքնարժեքի մոտ 15% աճը փոխհատուցվում է մարտկոցի կյանքի երկարացմամբ և ռիսկերի նվազեցմամբ:

ԱՇԽԱՏԱՆՔԻ ՀԻՄՆԱԿԱՆ ԱՐԴՅՈՒՆՔՆԵՐԸ

- Մշակվել է գաղտնագրման համակարգի արդյունավետության գնահատման մաթեմատիկական մոդել, որն ի տարբերություն առկա լուծումների՝ ինտեգրում է էներգասպառումը, հաշվարկային ցիկլերը և հիշողության սահմանա-փակումները: [1,2,6]
- Առաջարկվել են իրերի համացանցի սարքավորումների գաղտնագրման համար օգտագործվող բանալիների գեներացման, պահպանման և փոխանակման մեթոդներ, որոնք, ի տարբերություն առկա լուծումների, չեն պահանջում կենտրոնացված համակարգեր և հիմնված են ապարատային լուծման վրա: [3,4,7]
- Առաջարկվել է իրերի համացանցի սարքավորումների վիճակի և անվտանգության մակարդակի գնահատման մեթոդ, որն ի տարբերություն առկա լուծումների՝ կատարում է սարքավորման վարքագծի իրական ժամանակում վերլուծություն և հնարավորություն է տալիս՝ կատարելու հեռահար մշտադիտարկում:[5,8]

ՀՐԱՏԱՐԱԿՎԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐԸ

1. H.Minasyan “Enhancing zero trust architecture in IoT devices through hardware-accelerated cryptography” ՀԱՊՀ, Լրաբեր, Մաս 1, 2025 Էջ. 64-71
2. H.Minasyan “Systematic Security Evaluation of Comprehensive Hardware-Accelerated Key Management Framework for Cellular IoT” CSIT-2025, 2025, pp.175-177
3. Minasyan H.D., Naltakyan N.L. Batch As a Service with Enhanced Security for IOT-Enabled Smart Cities // Proceedings of NPUA: Information Technologies, Electronics, Radio Engineering.- 2025.- №2, P. 70-77.
4. N. Naltakyan, H. Minasyan "Federated Multi-Cluster Fog Architecture For Scalable IoT Key Management Using DANE/DANCE", 2025 IEEE East-West Design & Test Symposium (EWDTS), 2025
5. H.Minasyan."Performance Analysis and Security Evaluation of RFC 9783 PSA Attestation Tokens in Resource-Constrained IoT Environments", in 2026 IEEE International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA). Boracay Island, Philippines, 5–7 February. IEEE, pp. 2836-2841
6. H.Minasyan Mathematical modeling and quantitative security assessment of hardware-based cryptographic systems for resource-constrained IoT devices “Proceedings of The Republic of Armenia National Academy of Sciences and National Polytechnic University of Armenia Series of Technical Sciences” 2026 Volume 78 N 1 2025 pp. 79-86
7. H.Minasyan, Mari Yengoyan "Hardware-Accelerated 0-RTT TLS 1.3 for Resource-Constrained IoT Devices: Implementation and Security Analysis", Programming and Computer Software, vol. 52, no. 2, 2026
8. “Իրերի համացանցում սարքերի անվտանգ կառավարման համակարգ” ՀՀ Էկոնոմիկայի նախարարության մտավոր սեփականության գրասենյակ արտոնագրի հայտ AM20260032Y ՀԱՊՀ, Հ.Մինասյան, Ա.Պողոսյան 2026

MINASYAN HAMBARDZUM DAVIT

DEVELOPMENT OF METHODS AND TOOLS FOR ENSURING THE SECURITY OF INTERNET OF THINGS DEVICES

RESUME

The rapid development of Internet of Things (IoT) devices and the expansion of their application domains have led to the emergence of new cybersecurity challenges. Modern cyberattacks targeting the IoT ecosystem have become multi-layered and complex, whereas a significant portion of currently used devices either lacks built-in security mechanisms or relies on centralized cloud solutions. This reliance requires a constant connection, which is impractical in most real-world applications. The resource constraints inherent to IoT devices - in terms of computational power, memory, and energy consumption further complicate the application of traditional security approaches.

There is a fundamental contradiction between the strict requirements of information protection and the limited capabilities of IoT hardware. Although modern cellular IoT platforms (e.g., Nordic nRF9161) integrate hardware security modules (ARM CryptoCell-310, TrustZone), systematic methods for their efficient utilization throughout the device's entire lifecycle are lacking. At the same time, the recent publication of the RFC 9783 standard (PSA attestation token) creates an opportunity for evaluating device status, yet its applicability on resource-constrained devices has not been practically confirmed. The necessity of developing methods and tools aimed at solving the aforementioned problems justifies the relevance of this dissertation. Thus, the problem of developing encryption systems intended for Internet of Things devices is highly relevant both from the perspective of solving problems of scientific interest and designing systems that require automated control with practical significance.

Aim of the Work The aim of the work is to develop methods and tools to ensure the security of Internet of Things devices. To achieve this goal, the following tasks were set and solved:

- Develop a mathematical model for evaluating the cryptographic stability of IoT devices.
- Develop methods to ensure the generation, storage, and exchange of encryption keys.
- Develop a method for the real-time evaluation of the status and security level of IoT devices.

Practical Significance of the Work The developed solutions are applicable in smart homes, industrial automation, healthcare, and smart city infrastructures. The hardware-accelerated key management method significantly prolongs the lifespan of battery-operated

devices, which is cost-effective for sensors located in hard-to-reach places. Through the application of the developed collaborative architecture, key management ensures scalability for tens of thousands of devices.

Implementation of Results The key management and device status evaluation systems developed within the framework of the dissertation have been implemented in "RPE Controls LLC" to increase the security level of smart-controlled solutions. The mathematical model for evaluating the stability of the encryption process and its software implementation is used in the educational process of the "Information Security and Software Development" chair at the National Polytechnic University of Armenia.

The main results.

- A mathematical model for evaluating the efficiency of an encryption system has been developed, which, unlike existing solutions, integrates energy consumption, computational cycles, and memory constraints. [1,2,6]
- Methods for the generation, storage, and exchange of keys used for the encryption of Internet of Things (IoT) devices have been proposed, which, unlike existing solutions, do not require centralized systems and are based on a hardware solution. [3,4,7]
- A method for evaluating the state and security level of Internet of Things (IoT) devices has been proposed, which, unlike existing solutions, performs real-time analysis of device behavior and enables remote monitoring. [5,8]

МИНАСЯН АМБАРЦУМ ДАВИДОВИЧ

РАЗРАБОТКА МЕТОДОВ И ИНСТРУМЕНТОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

РЕЗЮМЕ

Стремительное развитие устройств Интернета вещей (IoT) и расширение сфер их применения привели к появлению новых проблем кибербезопасности. Современные кибератаки, нацеленные на экосистему IoT, стали многоуровневыми и сложными, в то время как значительная часть используемых в настоящее время устройств либо не имеет встроенных механизмов безопасности, либо опирается на централизованные облачные решения. Это требует постоянного соединения, что невыполнимо в большинстве реальных приложений. Ограничения ресурсов, характерные для устройств IoT - с точки зрения вычислительной мощности, памяти и энергопотребления - еще больше усложняют применение традиционных подходов к безопасности.

Существует фундаментальное противоречие между строгими требованиями к защите информации и ограниченными возможностями аппаратного обеспечения IoT. Хотя современные сотовые платформы IoT (например, Nordic nRF9161) интегрируют аппаратные модули безопасности (ARM CryptoCell-310, TrustZone), отсутствуют систематизированные методы их эффективного использования на протяжении всего жизненного цикла устройства. В то же время недавняя публикация стандарта RFC 9783 (токен аттестации PSA) создает возможность для оценки состояния устройств, однако его применимость на устройствах с ограниченными ресурсами на практике еще не подтверждена. Необходимость разработки методов и инструментов, направленных на решение вышеуказанных проблем, является обоснованием актуальности данной диссертационной работы. Таким образом, проблема разработки систем шифрования, предназначенных для устройств Интернета вещей, актуальна как с точки зрения решения проблем, представляющих научный интерес, так и с точки зрения проектирования систем, требующих автоматизированного управления и имеющих практическое значение.

Цель работы Целью работы является разработка методов и инструментов для обеспечения безопасности устройств Интернета вещей. Для достижения этой цели в работе были поставлены и решены следующие задачи:

- Разработать математическую модель оценки криптостойкости устройств Интернета вещей.
- Разработать методы обеспечения генерации, хранения и обмена ключами шифрования.

- Разработать метод оценки состояния и уровня безопасности устройств

Практическая значимость работы Разработанные решения применимы в инфраструктурах умных домов, промышленной автоматизации, здравоохранения и умных городов. Метод управления ключами с аппаратным ускорением значительно продлевает срок службы устройств, работающих от батарей, что экономически выгодно для датчиков, расположенных в труднодоступных местах. Благодаря применению разработанной совместной архитектуры управление ключами обеспечивает масштабируемость для десятков тысяч устройств.

Внедрение результатов Системы управления ключами и оценки состояния устройств, разработанные в рамках диссертации, внедрены в «Ар Пи И Контролс» (RPE Controls LLC) с целью повышения уровня безопасности интеллектуальных управляемых решений. Математическая модель оценки устойчивости процесса шифрования и ее программная реализация используются в учебном процессе кафедры «Информационная безопасность и программное обеспечение» Национального политехнического университета Армении.

Основные результаты.

- Разработана математическая модель оценки эффективности системы шифрования, которая, в отличие от существующих решений, учитывает энергопотребление, вычислительные циклы и ограничения памяти. [1,2,6]
- Предложены методы генерации, хранения и обмена ключами, используемыми для шифрования устройств Интернета вещей (IoT), которые, в отличие от существующих решений, не требуют централизованных систем и основаны на аппаратном решении. [3,4,7]
- Предложен метод оценки состояния и уровня безопасности устройств Интернета вещей (IoT), который, в отличие от существующих решений, выполняет анализ поведения устройства в реальном времени и позволяет осуществлять удаленный мониторинг. [5,8]