

ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ
ՊՐՈՔԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Ճաղարյան Գրիգոր Արշակի

**ԱՐԴՅՈՒՆԱՎԵՏ ՄԵԹՈՂՆԵՐԻ ԵՎ ԴՐԱՆՔ ԻՐԱԿԱՆԱՑՆՈՂ ԾՐԱԳՐԱՅԻՆ
ՀԱՄԱԿԱՐԳԻ ՄՇԱԿՈՒՄ ՆԱՆՈՉԱՓԱԿԱՆ ՀԻՇՈՂ ՍԱՐՔԵՐՈՒՄ
ԱՆՍԱՐՔՈՒԹՅՈՒՆՆԵՐԻ ՄՈԴԵԼԱՎՈՐՄԱՆ և ԹԵՍՏԱՅԻՆ
ԱԼԳՈՐԻԹՄՆԵՐԻ ԿԱՌՈՒՑՄԱՆ ՀԱՄԱՐ**

Ե. 13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի
մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ

Տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի
հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան – 2019

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И
АВТОМАТИЗАЦИИ НАН РА

Джагарян Григор Аршакович

**РАЗРАБОТКА ЭФФЕКТИВНЫХ МЕТОДОВ И РЕАЛИЗУЮЩИХ ИХ ПРОГРАММНЫХ
СИСТЕМ ДЛЯ МОДЕЛИРОВАНИЯ НЕИСПРАВНОСТЕЙ И ПОСТРОЕНИЯ ТЕСТОВЫХ
АЛГОРИТМОВ В НАНОМЕТРОВЫХ УСТРОЙСТВАХ ПАМЯТИ**

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

По специальности: 05.13.04 – математическое и программное обеспечение
вычислительных машин, комплексов, систем и сетей

Ереван – 2019

Ատենախոսության թեման հաստատվել է Երևանի Պետական Համալսարանում

Գիտական ղեկավար՝ տեխ. գիտ. դոկտոր Գ.Է. Հարությունյան

Պաշտոնական ընդդիմախոսներ՝ տեխ. գիտ. դոկտոր Հ.Հ. Հարությունյան
Ֆիզ.-մաթ. գիտ. թեկնածու Ա.Հ. Կոստանյան

Առաջատար կազմակերպություն՝
Երևանի մաթեմատիկական մեքենաների գիտահետազոտական ինստիտուտ

Պաշտպանությունը կայանալու է 2019թ. Մայիսի 7-ին, ժ. 16:00-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:
Սեղմագիրն առաքված է 2019թ. Մարտի 28-ին:

Մասնագիտական խորհրդի
գիտական քարտուղար, ֆիզ.-մաթ. գիտ. դոկտոր Հ.Գ. Սարուխանյան

Тема диссертации утверждена в Ереванском Государственном Университете

Научный руководитель: доктор технических наук Г.Э. Арутюнян

Официальные оппоненты: доктор технических наук Г.А. Арутюнян
кандидат физ.-мат. наук А.Г. Костанян

Ведущая организация:
Ереванский научно-исследовательский институт математических машин

Защита состоится 7-го мая 2019г. в 16:00 часов 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 28-го марта 2019г.

Ученый секретарь
специализированного совета, доктор физ.-мат. наук А.Г. Саруханян

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Ատենախոսության թեմայի արդիականությունը

Գորդոն Մուռը դեռևս քսաներորդ դարի 60-ական թվականներին կանխատեսել էր, որ տրանզիստորների քանակը ինտեգրալ սխեմաներում կրկնապատկվելու է յուրաքանչյուր 18 ամիսը մեկ¹: Ինտեգրալ սխեմայում տրանզիստորների քանակի աճին զուգահեռ փոքրանում է տրանզիստորի զբաղեցրած տարածքը և հետևաբար նաև տրանզիստորի չափերը: Ներկայումս աշխարհը թևակոխել է նանոտեխնոլոգիաների դարաշրջան, որտեղ տրանզիստորների դետալների չափերը չեն գերազանցում մի քանի տասնյակ նանոմետրը:

Տարիներ շարունակ տրանզիստորների MOSFET (metal-oxide-semiconductor field-effect transistor) տեխնոլոգիան հանդիսանում էր կիսահաղորդչային արդյունաբերությունում հիշող սարքերի պատրաստման համար օգտագործվող գերակայող տեխնոլոգիա: Այդ ընթացքում MOSFET տրանզիստորների չափերը մի քանի միկրոմետրից նվազելով հասել են մինչև 20 նանոմետրի²: Ցավոք տրանզիստորների չափերի փոքրացմանը զուգընթաց ի հայտ են եկել մի շարք բացասական երևույթներ, ինչպիսիք են կարճեցված-հոսքուղու և ավելցուկային հոսանքի հետ կապված խնդիրները, որոնք անհնարին են դարձրել MOSFET տրանզիստորների չափերի հետագա կրճատումը. ուստի կարիք է առաջացել լուծել խնդիրը անցում կատարելով այլընտրանքային տեխնոլոգիաների:

Որպես հավանական փոխարինող առաջարկված մի շարք տարբերակներից ամենամեծ հեղինակությունն է վայելում այսպես կոչված FinFET (fin field-effect transistor) տեխնոլոգիան, որի առանցքային գաղափարն է երկչափ (այլ կերպ ասած՝ հարթ) տրանզիստորներից անցում կատարելը դեպի եռաչափ տրանզիստորների³: FinFET տեխնոլոգիան MOSFET-ի համեմատությամբ շատ ավելի լավ բնութագրեր ունի հատկապես 20 նանոմետրի շերտ անցնելիս շնորհիվ նորարարական կառուցվածքի, ուստի իրավամբ այժմ համարվում է MOSFET-ի լիարժեք փոխարինողը: Աշխարհի մի շարք առաջատար ընկերություններ արդեն իսկ սկսել են սեփական հիշող սարքերի լայնածավալ արտադրությունը հիմնված FinFET տեխնոլոգիայի վրա^{4,5,6}: FinFET-ի հետ կապված հիմնական մարտահրավերներից մեկը հանդիսանում է այդ տեխնոլոգիայով նախագծված հիշող սարքերի թեստավորման և վերանորոգման խնդիրը: Չնայած

¹ G. E. Moore, "Cramming more components onto integrated circuits", Electronics, Volume 38, Number 8, April 1965.

² T.-J. King, "FinFETs for nanoscale CMOS digital integrated circuits", Proceedings of the IEEE/ACM International conference on Computer-aided design (ICCAD '05)", pp. 207-210, 2005.

³ R. Xie et al., "A 7nm FinFET technology featuring EUV patterning and dual strained high mobility channels", IEEE International Electron Devices Meeting, 2016, pp. 47-50.

⁴ Samsung, Press release, "Announces Mass Production of 2nd Generation 14-Nanometer FinFET Logic Process Technology", Jan. 2016.

⁵ Intel, "Opening New Horizons: 14 nm Process Technology", 2014.

⁶ A joint whitepaper from TSMC and Synopsys, "FinFET Technology – Understanding and Productizing a New Transistor", April 2013.

խնդրի կարևորությանը՝ մինչ այժմ քիչ աշխատանքներ են կատարվել այդ ուղղությամբ^{7,8,9}։ Այդ աշխատանքները հիմնականում տեսական բնույթ են կրել և ուղղված են եղել որոշակի ֆիզիկական թերությունների ուսումնասիրությանը, որոնք բնորոշ են FinFET հիշող սարքերին։ Սակայն փաստացիորեն չի տրվել գլխավոր երկու հարցերի պատասխանը՝ 1. արդյոք այդ ֆիզիկական թերությունները բերում են անսարքությունների նոր տիպերի առաջացմանը, որոնք կիրառելի չէին նախկին տեխնոլոգիաների դեպքում և 2. արդյոք այդպիսի անսարքությունները հայտնաբերվում են առկա թեստային լուծումների միջոցով, թե՛ կարիք կա մշակելու նոր լուծումներ։ Միայն այս երկու հարցերի պատասխանը իմանալով է հնարավոր FinFET հիշող սարքերի համար կառուցել արդյունավետ թեստային ալգորիթմներ, որոնք թույլ կտան ապահովել բարձր արտադրողական ելք։

Մյուս կարևոր խնդիրը, որը ծառայել է նանոչափական հիշող սարքերի թեստավորման ասպարեզում, արդի նանոչափական տեխնոլոգիաներով նախագծված ինտեգրալ սխեմաների թեստավորման միջավայրի ապահովության և անվտանգության (safety and security) խնդիրն է։ Վերջին շրջանում էլեկտրոնային համակարգերի լայնածավալ կիրառումը մի շարք ոլորտներում, այդ թվում «ավտոմոբիլային» (automotive) և «Իրերի Ինտերնետ» (Internet of Things) ոլորտներում մեծապես խստացրել է վերահսկողությունը այնտեղ օգտագործվող ինտեգրալ սխեմաների ապահովության, հուսալիության և անվտանգության խնդիրների նկատմամբ։ Դա վերաբերում է նաև այդ ինտեգրալ սխեմաների թեստավորման խնդրին։ Դժբախտաբար ներկայումս օգտագործվող թեստային լուծումները մեծամասամբ չեն կիրառում պաշտպանության մեխանիզմներ, ինչը կարող է հանգեցնել անվտանգության լուրջ խնդիրների և կարիք կա ցուցաբերել նոր մոտեցումներ այդ խնդիրները լուծելու համար։

Աշխատանքի նպատակն ու խնդիրները

Աշխատանքի նպատակն է հետազոտել արդի նանոչափական հիշող սարքերին բնորոշ անսարքությունները և կառուցել այդ անսարքությունները հայտնաբերող արդյունավետ թեստային լուծումներ, ինչպես նաև մշակել ինտեգրալ սխեմաների համար ներկառուցված թեստային համակարգի այնպիսի մոտեցում, որը կլուծի գոյություն ունեցող ապահովության և անվտանգության խնդիրները։

Հետազոտության օբյեկտը

Հետազոտման օբյեկտներ են հանդիսանում նանոչափական FinFET հիշող սարքերը, դրանց անսարքությունները և ինտեգրալ սխեմաներում թեստավորման ապահովության ու անվտանգության հիմնախնդիրները։

Հետազոտության մեթոդները

Աշխատանքում օգտագործված են դիսկրետ մաթեմատիկայի և օպտիմիզացիայի մեթոդները։

⁷ C.-W. Lin, M. C.-T. Chao, C.-C. Hsu, “Investigation of Gate Oxide Short in FinFETs and The Test Methods for FinFET SRAMs”, VLSI Test Symposium, 2013, pp. 1-6.

⁸ A. Karel et al., “Comparative study of Bulk, FDSOI and FinFET technologies in presence of a resistive short defect”, Latin-American Test Symposium, 2016, pp. 129-134.

⁹ R. Dibaj, D. Al-Khalili, M. Shams, “Comprehensive investigation of gate oxide short in FinFETs”, IEEE VLSI Test Symposium, 2017, pp. 1-6.

Արդյունքների գիտական նորությունը

- Փորձարկումների եղանակով կառուցվել են անսարքությունների ֆորմալ մոդելների նոր դասեր և ապացուցվել է, որ այդ մոդելները համապատասխանում են 16 և ավելի փոքր նանոմետրանոց FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ իրատեսական անսարքություններին:
- Կառուցվել են հենքային թեստային հաջորդականություններ՝ FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման համար:
- Կառուցվել են FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման և ախտորոշման արդյունավետ թեստային ալգորիթմներ:
- Արդի նանոչափական հիշող սարքերում անսարքությունների մոդելավորման և արդյունավետ թեստային ալգորիթմների ավտոմատ կառուցման համար մշակվել է համապատասխան ծրագրային միջավայր:
- Առաջարկվել են թեստավորման արդյունավետ լուծումներ ինտեգրալ սխեմաներում ապահովության և անվտանգության միջոցների համար:

Ստացված արդյունքների կիրառական նշանակությունը

Ստացված արդյունքները թույլ են տալիս հասնել FinFET հիշող սարքերում անսարքությունների ավելի մեծ ծածկույթի և դրա հետ մեկտեղ բարձրացնել թեստավորման արդյունավետությունը: Մինևույն ժամանակ հիշող սարքերի հետազոտման համար մշակված ավտոմատացված մեթոդը թույլ է տալիս արագացնել նոր տեխնոլոգիաներում անսարքությունների ուսումնասիրության գործընթացը:

Ներդրումներ

Հետազոտության արդյունքները ներդրվել են «Սինոփսիս» ընկերության ստատիկ նանոմետրանոց հիշող սարքերի թեստավորման գործիքներում և արդեն կիրառվում են նրա մի շարք հաճախորդ ընկերությունների կողմից:

Պաշտպանությանը ներկայացվում են հետևյալ դրույթները

- FinFET տեխնոլոգիայով նախագծված հիշող սարքերի համար կառուցված անսարքությունների ֆորմալ մոդելների նոր դասերը:
- Հենքային թեստային հաջորդականությունները՝ FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման համար:
- FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման և ախտորոշման արդյունավետ թեստային ալգորիթմները:
- Արդի նանոչափական հիշող սարքերում անսարքությունների մոդելավորման և արդյունավետ թեստային ալգորիթմների ավտոմատ կառուցման համար մշակված ծրագրային միջավայրը:
- Ինտեգրալ սխեմաներում ապահովության և անվտանգության միջոցների համար առաջարկված թեստավորման արդյունավետ լուծումները:

Ստացված արդյունքների ապրոբացիան

Աշխատանքի հիմնական արդյունքները և դրույթները գեկուցվել են մի շարք միջազգային գիտաժողովներում (VTS 2014, VTS 2015, EWDTs 2015, EWDTs 2016, EWDTs 2017, ICIT 2017, ITC 2017, ITC 2018), ինչպես նաև ԵՊՀ Տեղեկատվական տեխնոլոգիաների կրթական և հետազոտական կենտրոնի ընդհանուր սեմինարում:

Ատենախոսության արդյունքների փորձարկումը և հրապարակումները

Աշխատանքի հիմնական արդյունքները տպագրված են 12 աշխատություններում, որոնցից 11-ը՝ գիտական հոդվածներում, և 1-ը՝ շնորհված արտոնագրում: Հրապարակությունների ցուցակը բերված է սեղմագրի վերջում:

Ատենախոսության կառուցվածքը և ծավալը

Ատենախոսությունը բաղկացած է ներածության բաժնից, 4 գլուխներից, ամփոփումից, գրականության ցանկից և 3 հավելվածից: Աշխատանքի հիմնական մասը կազմում է 101 էջ, ունի 26 նկար և 17 աղյուսակ: Գրականության ցանկը զբաղեցնում է 10 էջ և ներառում է 104 աշխատություն: Աշխատանքի ընդհանուր ծավալը կազմում է 137 էջ:

Իմ երախտագիտությունն եմ հայտնում ՀՀ ԳԱԱ ակադեմիկոս, ֆ.մ.գ.դ., պրոֆեսոր Ս. Կ. Շուքուրյանին, ով իր օգտակար խորհուրդներով էապես նպաստել է աշխատանքի կայացմանը:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՄԱՌՈՏ ԲՈՎԱՆԴԱՎՈՒԹՅՈՒՆԸ

Ներածության բաժնում անդրադարձ է կատարվում թեմայի արդիականությանը, ոլորտում առկա մարտահրավերներին, ինչպես նաև ձևակերպված է աշխատանքի նպատակը և առաջարկվող լուծումների համառոտ նկարագրությունը:

Առաջին գլուխը սկսվում է համապատասխան գրականության վերլուծությամբ: Այնուհետև անդրադարձ է կատարվում ստատիկ նանոչափական հիշող սարքերին և նրանց թեստավորման հիմնական խնդիրներին: Հաջորդիվ ներկայացվում է FinFET տեխնոլոգիան, նրա հիմնական բնութագրերը և թեստավորման յուրահատկությունները:

Ստատիկ հիշող սարքեր: Հիշող սարքերը ինտեգրալ սխեմաների բաղկացուցիչ մաս են կազմում, որոնք նախատեսված են ինֆորմացիան գրանցելու, պահպանելու և վերարտադրելու համար: Առավել լայն կիրառություն ունեն ստատիկ հիշող սարքերը, որոնք նախատեսված են հատկապես ներդրված և բարձր արագությամբ աշխատող սխեմաների համար: Հիշող սարքերը բաղկացած են որոշակի քանակությամբ բջիջներից, որոնցից յուրաքանչյուրը կարողանում է պահպանել մեկ բիթ ինֆորմացիա: Հիշող սարքի բջիջը իր հերթին կազմված է 6 տրանզիստորներից: Այդ տրանզիստորներից 2-ը վերահսկում են բջջի մուտքը, իսկ մնացած 4-ը կազմում են հետադարձ հանգույցով միացված երկու ինվերտորներ նախատեսված բջջի արժեքը կայուն պահելու համար: Յուրաքանչյուր բջջում հնարավոր է իրարից անկախ գրել և կարդալ 0 կամ 1 արժեք: Հատկանշական է, որ ինտեգրալ սխեմայում գտնվող հիշող սարքերը վիճակագրորեն ավելի են հակված արտադրական անսարքությունների և պրոցեսի փոփոխման ազդեցությանը, հետևաբար այդ անսարքությունների

հայտնաբերումը գերագույն նշանակություն ունի բարձր օգտակար ելք ապահովելու տեսանկյունից:

Անսարքությունները հիշող սարքերում և նրանց դասակարգումը: Անսարքությունները նկարագրում են հիշող սարքերում առկա ֆիզիկական թերությունների արդյունքում բջիջների ոչ ճիշտ աշխատանքը: Ստատիկ հիշող սարքերում անսարքությունները սկսել են ակտիվորեն ուսումնասիրվել դեռևս վաղ 70-ական թվականներից¹⁰: Սկզբում դիտարկվում էին միայն ավանդական անսարքությունները՝ առանց գործողության (վիճակի) և մեկ գործողությամբ ակտիվացող: Այնուհետև հայտնաբերվեցին ավելի բարդ տիպի անսարքությունների դասեր՝ մեկից ավելի բջիջների և մեկից ավել գործողությունների կիրառման արդյունքում ակտիվացող: Հետևաբար՝ կարիք առաջացավ անսարքությունների դասակարգման, որի արդյունքում անսարքությունները բաժանվեցին մի քանի խմբերի: Առաջինը ըստ անսարքությունների քանակի կան կապակցված և չկապակցված անսարքություններ՝

- Չկապակցված անսարքությունները նրանք են, որոնցում միայն մեկ անսարքություն է մասնակցում,
- Կապակցված անսարքությունները համարվում են նրանք, որոնցում մասնակցում են երկու անսարքություններ, և դրանց զոհ բջիջները համընկնում են: Ընդ որում, եթե անսարքությունը մեկ բջջանոց է, ապա այն հանդիսանում է այդ անսարքության համար և՛ զոհ, և՛ ագրեսոր բջիջ:

Չկապակցված անսարքությունները իրենց հերթին բաժանվում են երկու խմբի ըստ անսարքությունը ակտիվացնող գործողությունների քանակի՝

- Անսարքությունները, որոնք ակտիվանում են միայն մեկ գործողության կիրառման արդյունքում, կոչվում են ստատիկ անսարքություններ,
- Անսարքությունները, որոնք ակտիվանում են երկու և ավելի գործողության հաջորդաբար կիրառման արդյունքում, կոչվում են դինամիկ անսարքություններ:

Ինչպես ստատիկ, այնպես էլ դինամիկ անսարքությունները իրենց հերթին բաժանվում են երկու ենթախմբի՝

- Մեկ բջջանոց անսարքություններ, երբ անսարքությունը առաջանում է նույն բջջի մեջ մեկ կամ ավելի գործողություն կիրառելու արդյունքում,
- Երկու բջջանոց անսարքությունները, երբ մեկ բջջի (որին անվանում են ագրեսոր բջիջ) վարքը ազդում է մեկ այլ բջջի (որին անվանում են զոհ բջիջ) արժեքի վրա:

Կապակցված անսարքությունները բաժանվում են երեք խմբի՝ ըստ այդ անսարքության կազմի մեջ մտնող երկու անսարքությունների տիպերի՝

- Երկու անսարքությունն էլ ստատիկ են,
- Անսարքություններից մեկը ստատիկ է, մյուսը՝ դինամիկ,
- Երկու անսարքությունն էլ դինամիկ են:

Ընդ որում, այդ անսարքություններից յուրաքանչյուրը կարող է լինել ինչպես մեկ բջջանոց, այնպես էլ երկու բջջանոց:

¹⁰ A.J. van de Goor, Testing semiconductor memories: Theory and Practice, John Wiley & Sons, Chichester, England, 1991.

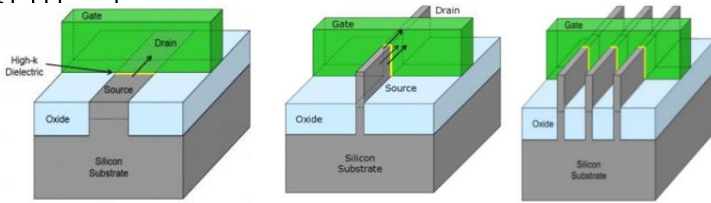
Թեստավորման հիմնական խնդիրները: Ստատիկ հիշող սարքերում անսարքությունների թեստավորումը հիմնականում կապված է երեք խնդրի հետ՝

- Անսարքությունների հայտնաբերում – պարզել՝ արդյոք հիշող սարքը պարունակում է անսարքություններ, թե՛ ոչ:
- Անսարքությունների տեղայնացում – պարզել հիշող սարքում անսարքություն պարունակող բջիջների հասցեները:
- Անսարքությունների ախտորոշում – պարզել հիշող սարքում առկա անսարքությունների տիպերը:

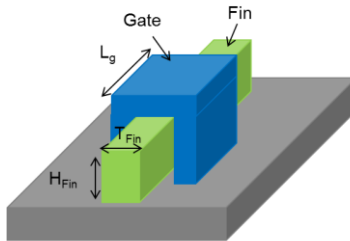
Ներկառուցված թեստավորումը և մարշ թեստի հասկացությունը: Ինտեգրալ սխեմաներում ներդրված ստատիկ հիշող սարքերի թեստավորումը սովորաբար իրականացվում է ներկառուցված թեստային համակարգերի (ՆԹՀ) միջոցով, որոնք ունեն մի շարք առավելություններ թեստավորման ժամանակի, զբաղեցրած տարածքի և բարձր օգտակար ելք ապահովելու տեսանկյունից: Հաշվի առնելով, որ թեստավորումը իրենից ներկայացնում է բավականին թանկ գործընթաց, և հիշող սարքերի թիվը ինտեգրալ սխեմաներում մեծ տեմպերով ավելանում է, ուստի ներկառուցված թեստային համակարգում հիմնականում օգտագործվում են գծային բարդության ալգորիթմներ, մասնավորապես՝ այսպես կոչված մարշ թեստեր: Մարշ թեստը իրենից ներկայացնում է մարշ էլեմենտների վերջավոր հաջորդականություն, որտեղ մարշ էլեմենտներից յուրաքանչյուրը բաղկացած է հասցեավորման կարգից՝ $\uparrow, \downarrow, \leftrightarrow$ (աճող, նվազող կամ ոչ էական) և վերջավոր թվով գրել/կարդալու գործողություններից՝ R0, R1, W0, W1 (գրել/կարդալ 0 կամ 1):

Արդի նանոչափական հիշող սարքեր: Մինչև քսան նանոմետրի սահմանաչափին հասնելը MOSFET տեխնոլոգիան համարվում էր կիսահաղորդչային արդյունաբերության մեջ գերակա տեխնոլոգիա, սակայն այնուհետև մի շարք բացասական երևույթների ի հայտ գալը ստիպեց մտածել այլընտրանքային տեխնոլոգիաներ փնտրելու մասին: Առաջարկվող տարբերակներից FinFET-ը իրեն շատ լավ դրսևորեց 16 նանոմետրից սկսած և այժմ համարվում է MOSFET-ի լիարժեք փոխարինողը: Նկար 1-ում պատկերված են MOSFET և FinFET տրանզիստորների կառուցվածքները: FinFET տրանզիստորների տարբերակիչ առանձնահատկությունն այն է, որ ղեկավարող հոսքուղին բաղկացած է բարակ ուղղահայաց կիսահաղորդչային «ֆիններից» (fins), որոնք շրջափակված են «փականի» (gate) էլեկտրոդներով՝ դրանով իսկ զգալիորեն մեծացնելով հոսքի ղեկավարման արդյունավետությունը: Ընդ որում, ինչքան շատ է ֆինների քանակը այնքան մեծ է հոսքի քանակը ակունքի (source) և հոսարանի (drain) միջև: FinFET տրանզիստորի նման տարածական կառուցվածքը լուծում է MOSFET-ին բնորոշ մի շարք խնդիրներ՝ արտահոսքի նվազեցում, կարճ հոսքուղու հետ կապված խնդիրների լուծում, բարելավված էլեկտրաստատիկ պարամետրեր և այլն: Նկար 2-ում պատկերված են FinFET տրանզիստորների հիմնական պարամետրերը, որոնք են՝ ֆինի բարձրությունը (H_{Fin}), ֆինի հաստությունը (T_{Fin}), փականի երկարությունը (L_g) և տրանզիստորի արդյունավետ լայնությունը ($T_{Fin+2*H_{Fin}}$): Ծնորհիվ FinFET տրանզիստորների յուրահատուկ տարածական կառուցվածքի նրանցում ի հայտ են գալիս նոր ֆիզիկական թերություններ, որոնք էլ իրենց հերթին հանգեցնում են նոր անսարքությունների առաջացմանը հիշող սարքերում: Նման անսարքությունները

հայտնաբերելու համար անհրաժեշտ է կիրառել նոր մոտեցումներ և կառուցել նոր թեստային ալգորիթմներ:



Նկար 1. MOSFET (ձախից), FinFET (կենտրոնում) և multifin FinFET (աջից) տրանզիստորների կառուցվածքը



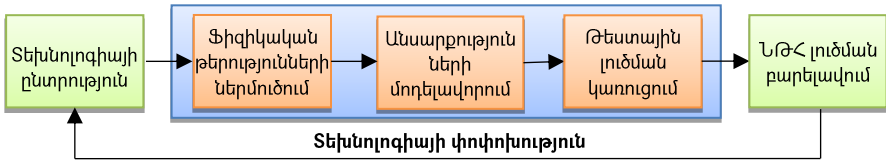
Նկար 2. FinFET տրանզիստորի հիմնական պարամետրերը

Երկրորդ գլուխը նկարագրում է FinFET տեխնոլոգիայի հիման վրա նախագծված հիշող սարքերի համար թեստային լուծման մշակման առաջարկվող մեթոդը սկսած ֆիզիկական թերությունների հետազոտումից մինչև արդյունավետ թեստային ալգորիթմների կառուցումը:

Ավանդական թեստավորման գործընթացը: Տարիների ընթացքում ներկառուցված հիշող սարքերի թեստավորման պահանջները անընդհատ փոփոխվել են տրանզիստորների տեխնոլոգիայի զարգացմանը զուգընթաց: Վերջին տարիներին այս գործընթացը հիմնականում կայունացել էր, քանի որ MOSFET տեխնոլոգիայի ընդարձակվելու ունակությունը թույլ էր տալիս շարունակաբար փոքրացնել տրանզիստորի չափերը առանց էապես փոփոխելու նրա վարքագիծը: Թեստավորման լուծման մշակման տիպային գործընթացը բաղկացած որոշակի քայլերի հաջորդականությունից պատկերված է նկար 3-ում, որը անհրաժեշտ է կատարել յուրաքանչյուր տեխնոլոգիայի փոփոխության հետ¹¹: Օգտագործելով նկարում պատկերված գործընթացը՝ MOSFET տեխնոլոգիային բնորոշ ֆիզիկական թերությունները մանրակրկիտ ուսումնասիրվել են, և մշակվել են համապատասխան անսարքությունների մոդելներ: Այնուհանդերձ, MOSFET տեխնոլոգիայի հասունացմանը զուգահեռ, հատկապես սկսած 65 նմ-ից մինչև 20 նմ, այս գործընթացը հիմնականում օգտագործվում էր թերությունների հայտնաբերման հավանականությունը որոշելու համար, քանի որ այլևս նոր անսարքություններ չէին հայտնաբերվում: Սակայն անցում կատարելով FinFET-ին այդ գործընթացը պետք է հիմնովին վերանայվի,

¹¹ R.-F. Huang, Y.-F. Chou, C.-W. Wu, “Defect oriented fault analysis for SRAM”, IEEE Asian Test Symposium (ATS), 2003, pp. 256-261.

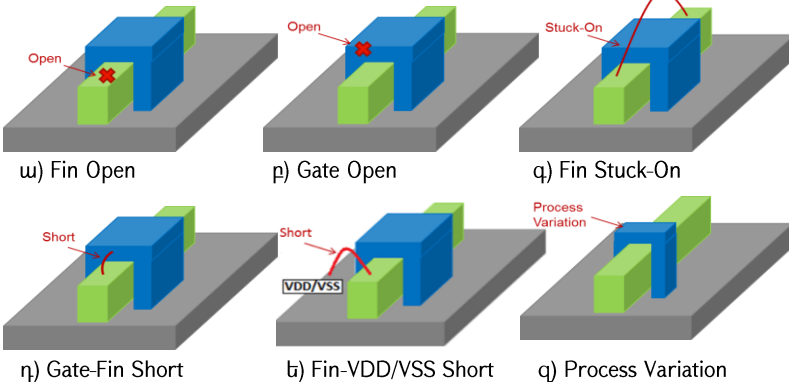
հատկապես, նկար 3-ում առանձնացված երեք հիմնական փուլերը՝ ֆիզիկական թերությունների ներմուծումը, անսարքությունների մոդելավորումը և թեստային լուծման կառուցումը՝ ներկայիս պահանջներին բավարարելու համար:



Նկար 3. Թեստային լուծման մշակման ավանդական ընթացակարգը

FinFET տեխնոլոգիայի համար դիտարկված ֆիզիկական թերությունները: Հետազոտության ընթացքում դիտարկվել են FinFET տեխնոլոգիային բնորոշ հետևյալ ֆիզիկական թերությունների մոդելները, որոնք պատկերված են նկար 4-ում՝

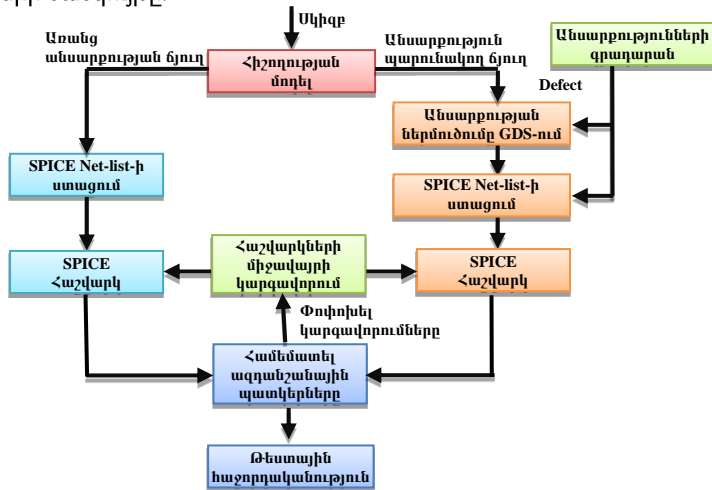
- ա) բացվածք ֆինի վրա (Fin Open),
- բ) բացվածք փականի վրա (Gate Open),
- գ) կարճ միացում տրանզիստորի ակունքի և հոսարանի միջև (Fin Stuck-On),
- դ) կարճ միացում փականի և ֆինի միջև (Gate-Fin Short),
- ե) կարճ միացում ֆինի և սնուցման լարման/հողակցման միջև (Fin-VDD/VSS Short),
- զ) տրանզիստորի պարամետրերի շեղում գործարանային արժեքներից (Process Variation):



Նկար 4. FinFET տեխնոլոգիայում դիտարկված ֆիզիկական թերությունների մոդելները

Առաջարկվող անսարքությունների մոդելավորման մեթոդը: Արդի հիշող սարքերի թեստավորման լուծման կառուցման գործընթացը համակարգված և քիչ ժամանակատար սարքելու համար մշակվել է անսարքությունների մոդելավորման ավտոմատացված մեթոդ ինչպես պատկերված է նկար 5-ում: Որպես մուտք, այն ստանում է ֆիզիկական թերությունների բազմություն (Defect LIB) և հաշվարկների միջավայրի կարգավորումները (Simulation Setup): Ֆիզիկական թերությունը ներմուծվում է հիշող սարքի GDS կամ SPICE Netlist մոդելում: Այնուհետև երկու SPICE հաշվարկներ են կատարվում (առանց ֆիզիկական թերության և ֆիզիկական թերության

անկայությամբ) և յուրաքանչյուր հաշվարկի համար հաջողությամբ կան անհաջողությամբ ավարտվելու ինֆորմացիա է ստացվում (PASS/FAIL), ինչպես նաև ստացվում են համապատասխան ազդանշանային պատկերները (waveforms): Եթե արդյունքը FAIL է, ապա գտնվել է առնվազն մեկ թեստային հաջորդականություն, որը հայտնաբերում է ֆիզիկական թերությունը, հակառակ դեպքում՝ համապատասխան կարգավորումները պետք է փոխվեն և հաշվարկը պետք է նորից կատարվի: Ստացված թեստային հաջորդականությունների հիման վրա անսարքությունների մոդելները ավտոմատ կերպով որոշվում են: Այդ հարցում մեծապես հղում է կատարվում անսարքությունների պարբերական աղյուսակին¹², որը թույլ է տալիս անսարքությունները ներկայացնել համակարգված ձևով և հեշտությամբ հայտնաբերել անհրաժեշտ անսարքությունների դասերը: Այն հետագայում օգտագործվում է նաև գնահատելու համար տրված թեստային ալգորիթմով հայտնաբերվող անսարքությունների ծածկույթը:

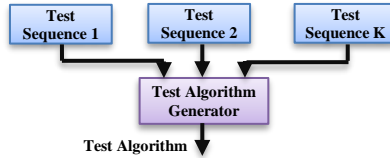


Նկար 5. Թեստային հաջորդականության և անսարքության մոդելի կառուցման մեթոդը

Անսարքությունների մոդելների և նրանց հայտնաբերող համապատասխան թեստային հաջորդականությունների կառուցումից հետո հաջորդ քայլը վերջնական թեստային ալգորիթմի կառուցումն է հիմնված այդ հաջորդականությունների վրա: Այդ գործընթացը նույնպես ավտոմատացված է: Ինչպես երևում է նկար 6-ից որպես մուտք ընդունվում են ստացված թեստային հաջորդականությունները և արդյունքում գեներացվում է արդյունավետ թեստային ալգորիթմ, որը ծածկում է դիտարկվող բոլոր անսարքությունները: Կարևոր է նաև նշել, որ կատարված փորձերը ցույց են տալիս, որ եթե որպես մուտք տրվող թեստային հաջորդականությունները նվազագույն

¹² G. Harutyunyan, S. Shoukourian, V. Vardanian, Y. Zorian, "An Effective Solution for Building Memory BIST Infrastructure Based on Fault Periodicity", IEEE VLSI Test Symposium, 2013, pp. 71-76.

երկարություն ունեն տվյալ անսարքությունների մոդելների հայտնաբերման առումով, ապա ստացված թեստային ալգորիթմը նույնպես ունենում է նվազագույն երկարություն:



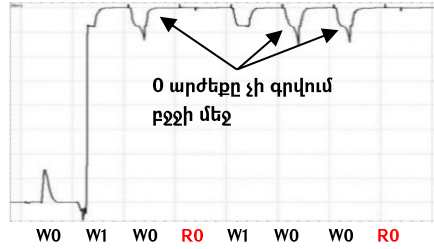
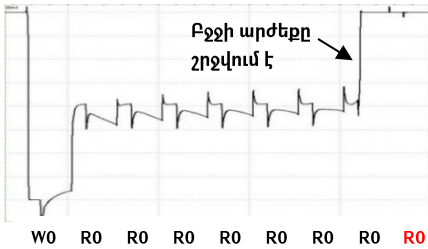
Նկար 6. Թեստային հաջորդականություններից թեստային ալգորիթմի կառուցման մեթոդը

Երրորդ գլուխը ամփոփում է լայնածավալ հետազոտության արդյունքները, որոնք ստացվել են FinFET հիշող սարքերում ֆիզիկական թերությունների ուսումնասիրության արդյունքում օգտագործելով վերևում նկարագրված մեթոդը:

Հետազոտության արդյունքների ամփոփում: Հետազոտության շրջանակներում առաջարկված մեթոդը կիրառվել է տարբեր նանոչափական FinFET տրանզիստորներից կազմված հիշող սարքերի վրա սկսած 16 նանոմետրից մինչև 7 նանոմետր: Կատարված SPICE հաշվարկների արդյունքները ցույց են տվել լուծման արդյունավետությունը և թույլ տվել կատարել բավականին կարևոր եզրակացություններ: Ուսումնասիրված ֆիզիկական թերություններից յուրաքանչյուրը ներմուծվել է հիշող սարքի տարբեր տրանզիստորներում առանձին-առանձին կամ մի քանիսում միաժամանակ: Համեմատականներ տանելու համար նմանատիպ ֆիզիկական թերություններ են ներմուծվել նաև MOSFET տեխնոլոգիայով կառուցված 28 և 45 նանոմետրանոց հիշող սարքերում: Ստացված ամենակարևոր արդյունքները հետևյալն են՝

- FinFET տեխնոլոգիայով նախագծված հիշող սարքերը ավելի հակված են դինամիկ անսարքությունների, քան MOSFET-ի դեպքում:
- FinFET տեխնոլոգիայով նախագծված հիշող սարքերը ավելի կայուն են պրոցեսի փոփոխման հետ կախված անսարքությունների նկատմամբ:
- Ստատիկ մեկ-բջջանոց և երկու-բջջանոց անսարքությունները բնորոշ են ինչպես FinFET, այնպես էլ՝ MOSFET հիշող սարքերին:

Նկար 7-ում ներկայացված են երկու տարբեր ֆիզիկական թերությունների արդյունքում հիշող սարքի հաշվարկների ազդանշանային պատկերները, որտեղից երևում է, որ այդ ֆիզիկական թերությունների հետևանքով հիշող սարքում առաջացել են երկու տարբեր տեսակի անսարքություններ: Առաջին դեպքում ռեգիստրի բացվածքի ներմուծումը տրանզիստորի ֆինի վրա հանգեցրել է հիշող սարքի բջջում 7 հաջորդական կարդալու գործողությամբ ակտիվացող dynamic Deceptive Read Destructive անսարքությանը (dDRDF0-7): Այդ անսարքության դեպքում 7-րդ կարդալու գործողությունը շրջում է բջջի արժեքը՝ առանց անհամապատասխանության մասին հաղորդելու, իսկ 8-րդ կարդալու գործողությունը՝ հայտնաբերում է անսարքությունը: Երկրորդ դեպքում ռեգիստրի բացվածք է ներմուծված տրանզիստորի փականի մեջ, որի արդյունքում հիշող սարքի բջջում ի հայտ է եկել Transistion Fault անսարքությունը: Հետազոտության արդյունքները ամփոփելիս պարզ դարձավ, որ հայտնաբերվել են որոշ դինամիկ անսարքությունների դասեր, որոնք բնորոշ են միայն FinFET տեխնոլոգիային:



Նկար 7. dDRDF-7 անսարքությունը (ծախից) և Transistion Fault անսարքությունը (աջից)

Այդ դասերը հետևյալն են՝

- Երեք և ավելի հաջորդաբար կարդալու գործողություններով ակտիվացող dynamic Read Destructive (dRDF) անսարքությունների դասը,
- Երեք և ավելի հաջորդաբար կարդալու գործողություններով ակտիվացող dynamic Deceptive Read Destructive (dDRDF) անսարքությունների դասը:

Տարբեր գործոնների ազդեցությունը անսարքությունների հայտնաբերելիության վրա:

FinFET տեխնոլոգիային բնորոշ անսարքությունները ուսումնասիրելիս պարզ դարձավ, որ թեստավորման միջավայրի տարբեր գործոնների (ջերմաստիճանի, լարման և հաճախության) արժեքը էական ազդեցություն ունի անսարքությունների ծածկույթի վրա: Փորձարկումների միջոցով կատարվեցին հետևյալ եզրակացությունները՝

- «Բացվածք» թերությունների դեպքում ջերմաստիճանի կամ լարման արժեքի բարձրացումը (նվազումը) հանգեցնում է հաջորդաբար կարդալու գործողությունների քանակի կրճատմանը (ավելացմանը), որոնք անհրաժեշտ են ակտիվացնելու համար dRDF/dDRDF անսարքությունները:
- «Կարճ միացում» թերությունների դեպքում ջերմաստիճանի կամ լարման արժեքի բարձրացումը (նվազումը) հանգեցնում է հաջորդաբար կարդալու գործողությունների քանակի ավելացմանը (կրճատմանը), որոնք անհրաժեշտ են ակտիվացնելու համար dRDF/dDRDF անսարքությունները:
- Ինչպես «Բացվածք», այնպես էլ «Կարճ միացում» թերությունների դեպքում հաճախության արժեքի բարձրացումը (նվազումը) հանգեցնում է հաջորդաբար կարդալու գործողությունների քանակի կրճատմանը (ավելացմանը), որոնք անհրաժեշտ են ակտիվացնելու համար dRDF/dDRDF անսարքությունները:

Հենքային թեստային հաջորդականություններ:

FinFET տեխնոլոգիային բնորոշ անսարքությունները հայտնաբերելու համար կառուցվել են մի քանի մարշ թեստային հաջորդականություններ, որոնք որպես հիմք կարող են ծառայել համապատասխան թեստային ալգորիթմներ կառուցելու գործում: Այդ հաջորդականությունները ունեն հետևյալ տեսքը՝

- TP1 – $\uparrow(R0, W1, R1^M)$;
- TP2 – $\uparrow(R1, W0, R0^M)$;
- TP3 – $\downarrow(R0, W1, R1^M)$;
- TP4 – $\downarrow(R1, W0, R0^M)$.

Որտեղ՝

- $M \geq 3$,
- R^M – M հատ հաջորդական Rx գործողություններ ($x = 0$ կամ 1),
- \uparrow – կիրառել թեստային գործողությունների հաջորդականությունը 0 հասցեում, հետո 1 հասցեում, ..., N հասցում (N –ամենամեծ հասցեն է),
- \downarrow – կիրառել թեստային գործողությունների հաջորդականությունը N հասցեում, հետո N-1 հասցեում, ..., 0 հասցեում:

Թեստային ալգորիթմներ: Մշակված թեստային հաջորդականությունների հիման վրա FinFET տեխնոլոգիայով նախագծված հիշող սարքերի համար կառուցվել են արդյունավետ թեստային ալգորիթմներ նրանց բնորոշ անսարքությունների հայտնաբերման և ախտորոշման համար, որոնք նկարագրված են ստորև՝

March FF

$\uparrow(W0)$;

$\uparrow(R0, W1, R1, R1, R1, R1, R1, R1, R1, R1)$; $\leftarrow TP1 - \uparrow(R0, W1, R1^M)$

$\downarrow(R1, W0, R0, R0, R0, R0, R0, R0, R0, R0)$; $\leftarrow TP4 - \downarrow(R1, W0, R0^M)$

$\downarrow(R0)$.

March FFD

$\downarrow(W0)$; $\downarrow(R0, W0)$; $\downarrow(R0)$;

$\downarrow(R0, W1, R1, R1, R1, R1, R1, R1, R1, R1)$; $\leftarrow TP3 - \downarrow(R0, W1, R1^M)$

$\uparrow(W0, R0)$; $\uparrow(R0, W1, R1, R1)$; $\downarrow(R1, W0, R0)$;

$\downarrow(R0, W1)$; $\downarrow(R1)$;

$\uparrow(R1, W0, R0, R0, R0, R0, R0, R0, R0, R0)$; $\leftarrow TP2 - \uparrow(R1, W0, R0^M)$

$\uparrow(R0)$; $\downarrow(W1, R1)$; $\uparrow(R1)$.

Գլուխ 4-ում ներկայացված են արդի տեխնոլոգիաներով կառուցված ինտեգրալ սխեմաներում ապահովության ու անվտանգության խնդիրները, անվտանգության ստանդարտների պահանջները և այդ պահանջներին բավարարող թեստավորման ճարտարապետության այնպիսի մոտեցում, որը լուծում է առկա խնդիրները:

Արդեն հայտնի փաստ է, որ ապահովությունը և անվտանգությունը 21-րդ դարի ամենակարևոր մարտահրավերներից են հանդիսանում: Այսօր էլեկտրոնային սարքերը կարելի է գտնել ամենուր, և դրա օգտագործման շուկաները բազմազան են, ներառյալ ռազմական և ավիացիոն ոլորտները, ինչպես նաև ավտոմոբիլային, բիո-բժշկական և այն: Սակայն խիստ մտահոգիչ է այն փաստը, որ վերջին տասնամյակների ընթացքում տեխնոլոգիաների աննախադեպ առաջընթացը չի ուղեկցվել ապահովության և անվտանգության ոլորտներում նույն չափի առաջընթացով: Կան բազմաթիվ վկայություններ, որոնք ցույց են տալիս, թե ինչպես համակարգի անվտանգության մեխանիզմների մեջ նույնիսկ ամենափոքր թերությունները կարող են չարամտորեն օգտագործվել՝ վտանգելով ամբողջ համակարգի անվտանգությունը:

Անվտանգության ստանդարտներ: Հաշվի առնելով ստեղծված իրավիճակը՝ վերջին շրջանում մշակվել են հստակ ստանդարտներ, որոնք փորձում են որոշակի կարգավորում մտցնել այդ ոլորտում: Մասնավորապես IEC 61508 ստանդարտը մշակվել է որպես ֆունկցիոնալ անվտանգության հիմնական ստանդարտ ցանկացած տեսակի էլեկտրոնային և էլեկտրական համակարգերի համար: Անվտանգությունը կարևոր նշանակություն ունի հատկապես ավտոմոբիլային ոլորտում, որը համարվում է

կիսահաղորդչային ոլորտում ներկայիս ամենաարագ զարգացող հատվածներից մեկը: Այս շուկայի համար արտադրվող ինտեգրալ սխեմաները պետք է լինեն առավելագույնս հուսալի և անվտանգ: Պահանջները, որոնց պետք է բավարարեն նշված ինտեգրալ սխեմաները նկարագրված են ավտոմոբիլային համակարգերի ֆունկցիոնալ անվտանգության ստանդարտում՝ ISO 26262-ում, որը իրականում IEC 61508 ստանդարտի հարմարեցումն է ավտոմոբիլային արդյունաբերության համար: ISO 26262 սահմանում է ավտոմեքենաների մեջ օգտագործման համար նախատեսված էլեկտրական և էլեկտրոնային համակարգերի համար ֆունկցիոնալ անվտանգության ընդունելի մակարդակի ապահովման պահանջները: Այդ պահանջներին բավարարելուց կախված, վերջնական արտադրանքը կարող է որակվել սահմանված ավտոմոբիլային անվտանգության ամբողջականության մակարդակներից մեկով՝ ASIL A-D: ASIL դասակարգումը օգտագործվում է ISO 26262-ի շրջանակներում արտահայտելու համար որոշակի վտանգի կանխման համար անհրաժեշտ ռիսկի նվազեցման մակարդակը: ASIL-D-ն հանդիսանում է որպես ամենաբարձր մակարդակ և ASIL-A՝ ամենացածր: ASIL-ը որոշվում է տեղի ունեցող կրիտիկական իրադարձության ժամանակ նրա բացահայտման հավանականության, վարորդի կողմից հնարավոր վերահսկելիության և հետևանքների հնարավոր ծանրության համադրությամբ: Այժմ ASIL սերտիֆիկացումը դարձել է կարևոր պահանջ ավտոմոբիլային արդյունաբերության համար որպես անվտանգության անհրաժեշտ մակարդակի առկայության երաշխիք:

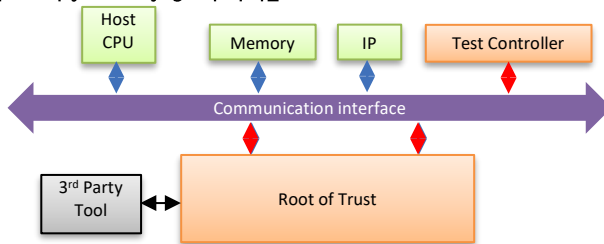
Ինտեգրալ սխեմաներում անվտանգության նկատառումները և սպառնալիքների դասակարգումը: Ինտեգրալ սխեմաների համար անվտանգ համակարգ նախագծելիս անհրաժեշտ է հաշվի առնել մի քանի կարևոր գործոններ, մասնավորապես՝ հստակեցնել պոտենցիալ հարձակվողների խմբերը, որոշել համակարգի կարևորագույն ակտիվները, հաշվարկել անվտանգության բյուջեն, ինչպես նաև դիտարկել հնարավոր բոլոր սպառնալիքների դասերը: Սովորաբար պոտենցիալ հարձակվողների երեք կարևոր խմբեր են քննարկվում՝ ներքին հարձակվողներ (Insiders), արտաքին հարձակվողներ (Outsiders) և պրոֆեսիոնալ կազմակերպություններ (Professional organizations): Այդ երեք դասերի ներկայացուցիչները տարբերվում են իրենց տեխնիկական գիտելիքներով, մասնագիտացված սարքավորումների առկայությամբ և այլն: Անվտանգ համակարգ կառուցելու մյուս կարևոր քայլը համակարգի կրիտիկական ակտիվների որոշումն է, որոնք անհրաժեշտ է պաշտպանել արտաքին միջամտությունից (օր.՝ գաղտաբառերը, օգտագործողների տվյալները, համակարգի բանալիները և այլն) և հաշվարկել դրա համար պահանջվող բյուջեն: Ընդ որում, խոսքը չի գնում միայն գումարի մասին, այլ նաև ծախսված ժամանակի ու պահանջվող աշխատուժի:

Վերջապես, կարևոր է հասկանալ հնարավոր սպառնալիքների միջավայրը ինտեգրալ սխեմաների յուրաքանչյուր փուլում, սկսած արտադրությունից մինչև վերջնական թեստավորում և շահագործում: Երեք հիմնական հարձակման դասերն են՝

- Հաղորդակցման հարձակումներ
 - Տվյալների հափշտակում (օր.՝ ծածկագրեր, բանալիներ և այլն)
 - Հեռակա հարձակումներ (օգտագործելով համակարգի «բացթողումները»)
- Ծրագրային հարձակումներ (օր.՝ վիրուսներ կամ լրտեսող ծրագրեր),
- Ֆիզիկական (ապարատային) հարձակումներ՝

- Ինտեգրալ սխեմայի պատյանից դուրս (օգտագործելով առկա ինտերֆեյսերը, թեստային պորտերը և այլ կողմնակի ուղիներ),
- Ինտեգրալ սխեմայի պատյանի ներսում (դեկապսուլյացիա, լազերային միջամտություն և այլն)

Անվտանգ թեստային լուծում ինտեգրալ սխեմաների համար: Ավանդական թեստային և վերանորոգման համակարգը ևս հանդիսանում է ինտեգրալ սխեմաների համար սպառնալիք ներկայացնող քանզի սովորաբար այն պաշտպանված չէ ոչ մի տեսակի հարձակումներից: Հասկապես հաշվի առնելով այն հանգամանքը, որ այսօր ավելի մեծ պահանջ կա թեստավորման լուծումների կիրառման համար սարքի միացման ընթացքում կամ նույնիսկ օգտագործման ռեժիմում, թեստավորման և օգտագործման ռեժիմների միջև անցումները օգտագործող հարձակումները դառնում են ավելի տարածված, քանի որ զգայուն տվյալները ավելի խոցելի են թեստային ռեժիմում: Այդ խնդիրը լուծելու համար առաջարկվում է ինտեգրալ սխեմայում ավելացնել այսպես կոչվող «Root of Trust» (RoT) մոդուլը, որը ստեղծում է վստահելի կատարողական միջավայր (Trusted Execution Environment) և հոգ է տանում համակարգում անվտանգության կարևորագույն գործառույթների կատարման համար՝ ներառյալ գաղտնի ծածկագրերի և այլ կարևոր տվյալների պաշտպանությունը, օգտագործողների նույնականացումը, անվտանգ հաղորդակցությունը և այլն: RoT-ն ոչ միայն պաշտպանում է համակարգը օգտագործման ռեժիմում, այլև վերահսկում է թեստային ռեժիմ մտնելիս նույնականացման և թեստավորման թույլտվություն ստանալու գործընթացները: Նկար 8-ում ցուցադրված է առաջարկվող ճարտարապետության հայեցակարգը:



Նկար 8. Ինտեգրալ սխեմայի ճարտարագիտությունը RoT մոդուլով

RoT մոդուլը վերահսկում է մուտքը ինտեգրալ սխեմայի ներսում բոլոր կարևոր մոդուլներին, այդ թվում նաև թեստային համակարգի (Test Controller): Երբ դիմում է լինում թեստային համակարգին, RoT-ն առանձին անվտանգ հաղորդակցման սեսիա է բացում, որի ընթացքում տեղի է ունենում նույնականացման գործընթացը հատուկ մշակված կրիպտոգրաֆիկ արձանագրության հիման վրա: Նույնականացման հաջող ավարտից հետո մուտքը թույլատրվում է և անվտանգ թեստավորման միջավայր է տրամադրվում նույն սեսիայի շրջանակներում: Այս մոտցումը թույլ է տալիս ոչ միայն ինտեգրալ սխեման պաշտպանել թեստային համակարգի շահագործումից եկող հնարավոր վտանգներից այլ նաև ապահովել որ իրականացվեն միայն այն թեստային և դիագնոստիկ ֆունկցիաները, որոնք լիազորված են RoT-ի կողմից:

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆՆԵՐ

Հետազոտության շրջանակներում՝

1. Փորձարկումների եղանակով կառուցվել են անսարքությունների ֆորմալ մոդելների նոր դասեր և ապացուցվել է, որ այդ մոդելները համապատասխանում են 16 և ավելի փոքր նանոմետրանոց FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ իրատեսական անսարքություններին [1], [2], [3], [4]:
2. Կառուցվել են հենքային թեստային հաջորդականություններ՝ FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման համար [5]:
3. Կառուցվել են FinFET տեխնոլոգիայով նախագծված հիշող սարքերին բնորոշ անսարքությունների հայտնաբերման և ախտորոշման արդյունավետ թեստային ալգորիթմներ [1], [4]:
4. Արդի նանոչափական հիշող սարքերում անսարքությունների մոդելավորման և արդյունավետ թեստային ալգորիթմների ավտոմատ կառուցման համար մշակվել է համապատասխան ծրագրային միջավայր [6], [7], [8]:
5. Առաջարկվել են թեստավորման արդյունավետ լուծումներ ինտեգրալ սխեմաներում ապահովության և անվտանգության միջոցների համար [9], [10], [11], [12]:

ԱՏԵՆԱՆՈՍՈՒԹՅԱՆ ԹԵՄԱՅՈՎ ՀՐԱՏԱՐԱԿՎԱԾ ԱՇԽԱՏՈՒԹՅՈՒՆՆԵՐ

1. G. Harutyunyan, G. Tshagharyan, V. Vardanian, Y. Zorian, “Fault Modeling and Test Algorithm Creation Strategy for FinFET-Based Memories”, IEEE VLSI Test Symposium (VTS), USA, 2014, pp. 49-54.
2. G. Harutyunyan, G. Tshagharyan, Y. Zorian, “Test & Repair Methodology for FinFET-Based Memories”, IEEE Transactions on Device and Materials Reliability, Vol. 15, No. 1, March 2015, pp. 3-9.
3. G. Harutyunyan, G. Tshagharyan, Y. Zorian, “Impact of Parameter Variations on FinFET Faults”, IEEE VLSI Test Symposium (VTS), USA, 2015, pp. 145-148.
4. G. Tshagharyan, G. Harutyunyan, S. Shoukourian, Y. Zorian, “Overview Study on Fault Modeling and Test Methodology Development for FinFET-Based Memories”, IEEE East-West Design and Test Symposium (EWDTS), Georgia, 2015, pp. 19-22.
5. G. Tshagharyan, G. Harutyunyan, S. Shoukourian, Y. Zorian, “FinFET-Based Memory Testing Using Multiple Read Operations”, Patent Application, No. 15/718,284, Filed on September 28, 2017.
6. G. Tshagharyan, “Built-In Test Flow for FinFET-based Memory Devices”, Reports of National Academy of Science, Armenia, 2015, Vol. 115, No 4, pp.276-283.
7. G. Tshagharyan, G. Harutyunyan, Y. Zorian, A. Gebregiorgis, M. S. Golanbari, R. Bishnoi and M. B. Tahoori, “Modeling and Testing of Aging Faults in FinFET Memories for Automotive Applications”, IEEE International Test Conference (ITC), USA, 2018, Paper Auto 3.1, pp. 1-10.
8. S.M. Nair, R. Bishnoi, M. B. Tahoori, G. Tshagharyan, H. Grigoryan, G. Harutyunyan and Y. Zorian, “Defect injection, Fault Modeling and Test Algorithm Generation Methodology for STT-MRAM”, IEEE International Test Conference (ITC), USA, 2018, Paper S 5.1, pp. 1-9.
9. G. Tshagharyan, G. Harutyunyan, S. Shoukourian, Y. Zorian, “Securing Test Infrastructure of System-on-Chips”, IEEE East-West Design and Test Symposium (EWDTS), Armenia, 2016, pp. 29-32.
10. G. Harutyunyan, S. Shoukourian, G. Tshagharyan, “Security Issues in Test and Repair Infrastructure for Systems-on-Chip”, International Conference in Information and Communication Technologies (ICIT), Russia, 2017, pp. 114-122.
11. G. Tshagharyan, G. Harutyunyan, S. Shoukourian, Y. Zorian, “Experimental study on Hamming and Hsiao Codes in the Context of Embedded Applications”, IEEE East-West Design and Test Symposium (EWDTS), Serbia, 2017, pp. 25-28.
12. G. Tshagharyan, G. Harutyunyan, Y. Zorian, “An Effective Functional Safety Solution for Automotive Systems-on-Chip”, IEEE International Test Conference (ITC), USA, 2017, Paper ET 2.2, pp. 1-10.

RESUME

GRIGOR ARSHAK TSHAGHARYAN

DEVELOPMENT OF EFFICIENT METHODS AND SOFTWARE SYSTEM FOR FAULT MODELING AND TEST ALGORITHM CONSTRUCTION IN NANO-SCALE MEMORY DEVICES

Introduction

For many years planar MOSFET was the prevailing transistor technology for the construction of memory devices. Nevertheless, growing short-channel and current leakage problems of this type of transistors make it almost impossible to continue further scaling down the feature sizes below 20nm without negative consequences. Thereby, several alternative approaches have been proposed recently among which FinFET technology is considered as having all the necessary preconditions to become MOSFET successor. FinFET transistors have unique structure with vertical silicon fins wrapped by gate electrodes, which replace the conventional transistor channel and provide significant improvement over the MOSFET. Due to the structural differences between the FinFET and MOSFET, conventional test algorithms may not be sufficient to cover the whole spectrum of possible defects in FinFET-based memories. Despite the importance of the problem, only relatively small number of research activities have been done in this area so far. These works were mainly of theoretical nature and were aimed at studying some of the physical defects typical to FinFET memory devices. Meanwhile, the two main questions have in fact remained unanswered: 1) whether there are faults specific to FinFET-based memories and 2) whether these types of faults can be detected by existing test solutions or new test algorithms must be developed.

The second problem which has arisen in the field of embedded memory testing is the safety and security of test architecture on System-on-Chips (SoCs). Widespread utilization of electronic systems in number of fields, including automotive and Internet of Things (IoT), has greatly increased the stress of safety, reliability, and security problems within such SoCs. Unfortunately, presently used test solutions have many weaknesses which can result into serious security issues and new approaches are required with this regard.

The aim of the thesis

The purpose of the work is to investigate the faults specific to modern memory devices and to build efficient test solutions for detecting these faults as well as to develop a built-in test system concept for SoCs that will address existing safety and security issues.

Scientific novelty

- New classes of formal fault models are constructed in an experimental way and proved that these models match sub 16 nanometer FinFET technology specific realistic defects.

- Basic test patterns are constructed for detection of FinFET-specific memory faults.
- New efficient test algorithms are constructed for detection and diagnosis of FinFET-specific memory faults.
- The corresponding software environment is developed for fault modeling and efficient test algorithms construction in an automatic way in modern nano-scale memory devices.
- Efficient test solutions are proposed for security and safety means in System-on-Chips.

Practical value and implementation

The obtained results allow to achieve a greater fault coverage in FinFET-based memory devices and simultaneously increase the testing efficiency. At the same time, an automated flow developed for memory devices allows to speed up the process of fault investigation in new technologies.

The results of the research have been embedded in the Synopsys STAR Memory System tool for testing static nanoscale memory devices and are already being used by number of customer companies.

The following theses are presented for defense

- New classes of formal fault models built for FinFET-based memory devices [1], [2], [3], [4].
- Basic test sequences for detection of FinFET-specific memory faults [5].
- Efficient test algorithms for detection and diagnosis of FinFET-specific memory faults [1], [4].
- Software environment developed for fault modeling and automatic construction of efficient test algorithms in modern nano-scale memory devices [6], [7], [8].
- Efficient test solutions for safety and security means in integrated circuits [9], [10], [11], [12].

ДЖАГАРЯН ГРИГОР АРШАКОВИЧ

РАЗРАБОТКА ЭФФЕКТИВНЫХ МЕТОДОВ И РЕАЛИЗУЮЩИХ ИХ ПРОГРАММНЫХ СИСТЕМ ДЛЯ МОДЕЛИРОВАНИЯ НЕИСПРАВНОСТЕЙ И ПОСТРОЕНИЯ ТЕСТОВЫХ АЛГОРИТМОВ В НАНОМЕТРОВЫХ УСТРОЙСТВАХ ПАМЯТИ

Введение

На протяжении многих лет плоский MOSFET был преобладающей транзисторной технологией для производства устройств памяти. Тем не менее, растущие проблемы с короткими каналами и утечкой тока в этих типов транзисторов делают практически невозможным дальнейшее уменьшение размеров транзисторов ниже 20 нанометров без негативных последствий. В связи с этим, было предложено несколько альтернатив, среди которых технология FinFET является наиболее популярной. Транзисторы FinFET имеют уникальную структуру с вертикальными “финами” обернутыми электродами “затвора”, которые заменяют обычный транзисторный канал и обеспечивают улучшенные характеристики по сравнению с MOSFET. Из-за структурных различий между FinFET и MOSFET традиционные тестовые алгоритмы могут быть недостаточными для тестирования устройств памяти на основе FinFET. Несмотря на важность проблемы, в настоящее время сравнительно небольшое количество исследований было проведено в этой области, которые в основном были сосредоточены на локальных проблемах. Между тем, два основных вопроса остаются неотвеченными: 1) существуют ли неисправности специфичные для устройств памяти на основе FinFET, и 2) могут ли этого типа неисправности быть обнаружены существующими тестовыми решениями или есть необходимость разработки новых тестовых алгоритмов.

Вторая проблема, возникшая в области тестирования встроенных устройств памяти – это безопасность и надежность тестового решения использующийся в интегральных схемах. Широкое использование электронных систем в различных областях, таких как автомобилестроение и “Интернет вещей”, привлекло внимание к проблемам безопасности и надежности в таких системах. К сожалению, используемые тестовые решения имеют множество недостатков, которые могут привести к серьезным проблемам безопасности, и в связи с этим требуются новые подходы и решения.

Цели работы

Целью работы является исследование неисправностей, характерных для современных устройств памяти, и создание эффективных тестовых решений для обнаружения этих неисправностей, а также разработка концепции тестовой архитектуры для интегральных схем, которая решит существующие проблемы безопасности и надежности.

Научная новизна

- Были сконструированы новые классы формальных моделей неисправностей и было доказано, что эти модели соответствуют реальным неисправностям специфичным для 16 нанометровых и меньших устройств памяти на основе FinFET.
- Были сконструированы базовые тестовые шаблоны для обнаружения неисправностей специфичные для устройств памяти на основе FinFET.
- Были созданы новые эффективные алгоритмы для обнаружения и диагностики такого рода неисправностей.
- Разработана соответствующая программная среда для моделирования неисправностей и автоматического построения эффективных алгоритмов тестирования в современных нанометровых устройствах памяти.
- Предложены эффективные тестовые решения для средств защиты и безопасности в интегральных схемах.

Практическая ценность и реализация

Полученные результаты позволяют добиться большего покрытия неисправностей для устройств памяти на основе FinFET и одновременно повысить эффективность тестирования. В то же время программная система, разработанный для устройств памяти, позволяет ускорить процесс исследования неисправностей в новых технологиях.

Результаты исследования были внедрены в инструмент STAR Memory System компании Synopsys для тестирования статических нанометровых устройств памяти и уже используются рядом компаний-клиентов.

На защиту представлены следующие положения

- Новые классы формальных моделей неисправностей, построенные для устройств памяти на основе FinFET [1], [2], [3], [4].
- Базовые тестовые шаблоны для обнаружения неисправностей специфичные для устройств памяти на основе FinFET [5].
- Эффективные алгоритмы тестирования для обнаружения и диагностики неисправностей специфичные для устройств памяти на основе FinFET [1], [4].
- Программная среда для моделирования неисправностей и автоматического построения эффективных алгоритмов тестирования в современных нанометровых устройствах памяти [6], [7], [8].
- Эффективные тестовые решения для средств защиты и безопасности в интегральных схемах [9], [10], [11], [12].