ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Դանոյան Դավիթ Հակոբի

ԱՆՎՏԱՆԳ ԲԱԶՄԱՄԱՍՆԱԿԻՑ ՀԱՇՎԱՐԿՆԵՐ ՀԻՄՆՎԱԾ ՆՈՐ ԱՆՏԵՂՅԱԿ ՓՈԽԱՆՑՄԱՆ ՀԱՂՈՐԴԱԿԱՐԳԻ ՎՐԱ

Ե.13.05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ և ծրագրերի համալիրներ» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

Երևան – 2016

INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS OF NAS RA

Davit Hakob Danoyan

SECURE MULTI-PARTY COMPUTATIONS BASED ON A NOVEL OBLIVIOUS TRANSFER PROTOCOL

ABSTRACT

For obtaining candidate degree in technical sciences in specialty 05.13.05 “Mathematical modeling, numerical methods and software complexes”

Yerevan - 2016

Ատենախոսության թեման հաստատվել է Երևանի պետական համալսարանում

Գիտական ղեկավար՝	տեխ.գիտ.դոկտոր	Գ.Հ. Խաչատրյան
Պաշտոնական ընդդիմախոսներ՝	ֆիզ.մաթ.գիտ.դոկտոր	Լ.Հ. Ասլանյան
	ֆիզ.մաթ.գիտ.թեկնածու	Ս.Ե. Աբրահամյան
Առաջատար կազմակերպություն՝	Հայ-Ռուսական (Սլավոնական) Համալսարան	

Պաշտպանությունը կայանալու է 2016թ. հունիսի 8-ին, ժ. 16:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ-ի գրադարանում:
Սեղմագիրը առաքված է 2016թ. մայիսի 7-ին:

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

The subject of the dissertation has been approved in the Yerevan State University.

Scientific advisor:	Doctor of Tech. Sci.	G. H. Khachatryan
Official opponents:	Doctor of Phys. Math. Sci.	L. H. Aslanyan
	Candidate of Phys. Math. Sci.	S.Y. Abrahamyan
Leading organization:	Russian-Armenian (Slavonic) University	

The defense of thesis will take place on 8 June, 2016 at 16:00 in Institute for Informatics and Automation Problems of NAS RA, during the session of the specialized council 037 “Informatics and Computing Systems”, address: 0014, Yerevan, P. Sevak str. 1.

The thesis is available in library of IIAP of NAS RA.
The abstract is sent on 7 May 2016.

Scientific Secretary of the specialized council
Doctor of Phys. Math. Sci.  H.G.Sarukhanyan

Աշխատանքի ընդհանուր բնութագիրը

Թեմայի արդիականությունը

Ժամանակակից գաղտնագրության կարևոր խնդիրներից է մի քանի կողմերի մուտքային տվյալների գաղտնիությունը պահպանող հաշվարկների իրականացումը: Դիցուք n թվով միմյանց չվստահող $P_1, \dots, P_n$ կողմերը ցանկանում են հաշվարկել նախապես ընտրված մի ֆունկցիա, որում յուրաքանչյուր մասնակից ունի իր գաղտնիք հանդիսացող մուտքային տվյալները: Կարևոր պայման է յուրաքանչյուր մասնակցի մուտքային տվյալների գաղտնիության պահպանումը այլ մասնակիցներից կամ մասնակիցների խմբերից, այսինքն հաշվարկի իրականացման արդյունքում որևէ մասնակցի մուտքային տվյալների մասին հայտնի դարձած տեղեկությունները չպետք է լինեն ավելին, քան միայն ֆունկցիայի ելքային տվյալներից դուրս բերվող տեղեկությունները:

Ֆունկցիայի՝ մուտքային տվյալների գաղտնիությունը պահպանող հաշվարկի իրականացումը վստահելի կողմի մասնակցությամբ կարելի է կազմակերպել տրամադրելով գաղտնի տվյալները վստահելի կողմին, ով կիրականացնի ֆունկցիայի հաշվարկը և արդյունքը կտրամադրի մասնակիցներին, առանց բացահայտելու յուրաքանչյուրի տվյալները: Այս դեպքում սակայն առաջանում են անվտանգության խնդիրներ, քանի որ գաղտնիքների կենտրոնացումը հնարավորություն է ընձեռում բացահայտել տեղեկություններ բոլորի մուտքային տվյալների մասին՝ գրոհելով միայն վստահելի մասնակցին: Մյուս կողմից որոշ հաշվարկների դեպքում վստահելի կողմերի առկայությունը կամ այդպիսիքին տվյալների տրամադրումը անթույլատրելի է օրենսդրական մակարդակով՝ պայմանավորված մուտքային տվյալների հույժ գաղտնիությամբ: Այդպիսի դեպքերից են բժշկական հաստատությունների հնարավոր համագործակցությունները, որոնց ընթացքում իրականացվող հաշվարկներում օգտագործվում են մարդկանց բժշկական պատմությունները կամ կենսաչափական տվյալները: Վստահելի կողմից խուսափելու մեկ այլ հիմնանավորում է վերջինիս կողմից գաղտնի տվյալների գործածման կանխումը տնտեսական առավելություն ստանալու կամ կողնապահության նպատակով առցանց աճուրդների կամ մրցակցող անհատների կամ կազմակերպությունների համագործակցության դեպքերում:

Անվտանգ բազմամասնակից հաշվարկներ (ԱԲՀ) իրականացնող հաղորդակարգերի հետազոտությունները երկար ժամանակ միայն տեսական բնույթ էին կրում, սակայն վերջին տասնամյակում իրականացվել են անվտանգ հաշվարկներ իրականացնող մի քանի ծրագրային համալիրներ, որոնք հիմնված են տարբեր հաղորդակարգերի վրա: ԱԲՀ-ի առաջին իրական կիրառումը կայացավ 2008-ին Դանիայում անցկացվող աճուրդի ընթացքում: Նման համակարգերի կիրառությունները ներկայացվել են նաև էլեկտրոնային ընտրությունների, առցանց առևտրի, գենոմի հետազոտությունների և

այլ ոլորտներում: 2012 Չոին և այլոք ներկայացրել են այսպես կոչված GMW հաղորդակարգի վրա հիմնված մի համակարգ, որը հանդիսանում էր ԱԲՀ լավագույն իրականացումը հիմնված անտեղյակ փոխանցման (oblivious transfer) հաղորդակարգի վրա: Անտեղյակ փոխանցման հաղորդակարգերի ոլորտում նոր զարգացումների կիրառումը հնարավոր է դարձնում վերոնշյալ համակարգի արդյունքների էապես բարելավումը:

<u>Աշխատանքի նպատակը</u>

Աշխատանքի գլխավոր նպատակն է կառուցել ծրագրային համալիր, որը թույլ է տալիս մի քանի կողմերի իրականացնել հաշվարկներ հիմնված կողմերի գաղտնի մուտքային տվյալների վրա ՝ առանց բացահայտելու այդ տվյալները և էապես բարելավել նախկինում իրականացված նմանատիպ համակարգերի արագագործությունը, խուսափելով բաց բանալիով գաղտնագրության գործողություններից և փոխարենը օգտագործելով սպիտակ արկղի գաղտնագրության (white-box cryptography) վրա հիմնված անտեղյակ փոխանցումներ: Ցանկալի է նաև պարզեցնել օգտագործողների աշխատանքը համակարգի հետ՝ ներառելով այնտեղ բարձր մակարդակի ծրագրավորման լեզվից բուլյան սխեմա կառուցող կոմպիլյատոր, որն օգտագործողին ազատում է սխեմա կառուցելու խնդրից և հաշվի է առնում տվյալ համակարգի առանձնահատկությունները:

<u>Հետազոտման մեթոդները</u>

Աշխատանքում օգտագործվել են սպիտակ արկղի գաղտնագրության մեթոդներ, սիմետրիկ բանալիով գաղտնագրության մեթոդներ և ծրագրային ապահովման նախագծման մեթոդներ:

<u>Գիտական նորույթը</u>

- Սպիտակ արկղի գաղտնագրության կիրառում անվտանգ բազմամասնակից հաշվարկների իրականացման համար
- Սպիտակ արկղով անտեղյակ փոխանցման հաղորդակարգի ընդլայնման կառուցում
- Գրականության մեջ հայտնի (այսպես կոչված GMW) հաղորդակարգի ընդլայնման կառուցում, որը թույլ է տալիս մուտքային և ելքային տվյալներ ունեցող, սակայն հաշվարկմանը չմասնակցող կողմերի ներառում

<u>Աշխատանքի արդյունքների հավաստիությունը</u> հիմնավորվում է իրականացված ծրագրային համակարգի կիրառմամբ ստացված մի շարք փորձնական արդյունքներով:

Ստացված արդյունքների կիրառական նշանակությունը

Ատենախոսության շրջանակներում նախագծվել և իրականացվել է ծրագրային համակարգ, որը

- ներառում է վերջին տարիներին առաջարկված տարբեր տեսական մեթոդների ծրագրային իրականացումներ և հետազոտողին հնարավորություն է տալիս կատարել տարատեսակ փորձարկումներ դրանց հետ, ինչպես նաև գործնականում հաշվարկել նոր մշակվող մոտեցումների արդյունավետության տարատեսակ բնութագրիչներ
- օգտագործողներին հնարավորություն է տալիս նկարագրել մուտքային տվյալների օգտագործմամբ կատարկող հաշվարկներ և կարող է օգտագործվել ԱԲՀ պահանջող գործնական կիրառություններում

Աշխատանքի արդյունքների ներդրումը

Աշխատանքի արդյունքում ստեղծված ծրագրային համակարգը ներդրվել է «Շանթ Քոմփյու» ՍՊԸ-ի կողմից, «Այ Փի Էս Սի» Քաղաքական և սոցիոլոգիական խորհրդատվությունների ինստիտուտ ՍՊԸ-ի պատվերի շրջանակներում մշակվող անանուն վարկանիշային համակարգում և գտնվում է փորձնական շահագործման փուլում:

Պաշտպանությանը ներկայացվող դրույթները

- Նախագծվել և իրականացվել է անվտանգ բազմամասնակից հաշվարկների համակարգ, որն ունի էապես բարելավված արդյունավետություն նախկին իրականացումների համեմատ:
- Կառուցվել է սպիտակ արկղով անտեղյակ փոխանցման հաղորդակարգի ընդլայնում, որը թույլ է տալիս նվազեցնել անհրաժեշտ անտեղյակ փոխանցումների քանակը:
- Իրականացվել է մուտքային ֆունկցիայի բարձր մակարդակի լեզվով նկարագրությունից բուլյան սխեմա կառուցող կոմպիլյատոր՝ հաշվի առնելով GMW հաղորդակարգի առանձնահատկությունները:

Աշխատանքի արդյունքները զեկուցվել են

Ատենախոսության հիմնական արդյունքներն ու դրույթները զեկուցվել և քննարկվել են

- ՀԱՀ «Applied Cryptography Laboratory» հետազոտական լաբորատորիայի սեմինարների ընթացքում (2013-2016 թթ., ք. Երևան)
- ԵՊՀ Ինֆորմատիկայի և կիրառական մաթեմատիկայի ֆակուլտետի սեմինարների ընթացքում (2013-2016 թթ., ք. Երևան)
- «Computer Science and Information Technologies» 10-րդ միջազգային գիտաժողովում (CSIT, 2015 թ., ք. Երևան)

- Հայ-Ռուսական (Սլավոնական) Համալսարանի 10-տարեկան գիտական ժողովի ընթացքում (2015 թ., ք. Երևան)
- ՀՀ ԳԱԱ ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի ընդհանուր սեմինարում

Հրապարակումներ

Ատենախոսության հիմնական արդյունքները տպագրված են 4 գիտական աշխատություններում, որոնք թվարկված են սեղմագրի վերջում:

Աշխատանքի կառուցվածքը և ծավալը

Ատենախոսությունը բաղկացած է ներածությունից, 3 գլուխներից, ամփոփումից և օգտագործված գրականության ցանկից: Աշխատանքի ընդհանուր ծավալն է 103 էջ՝ ներառյալ 92 անուն օգտագործված գրականության ցանկում:

Աշխատանքի բովանդակությունը

Ներածության բաժնում հիմնավորված է հետազոտության արդիականությունը և բերված են կիրառական նշանակությունը հաստատող փաստեր: Նաև հակիրճ ներկայացված են ոլորտում առկա ժամանակակից խնդիրները և մոտեցումները, բերված են գործնական կիրառությունների օրինակներ, ձևակերպված են հետազոտության հիմնական նպատակները և ընգծված են աշխատության գիտական նորույթ հանդիսացող դրույթները:

Առաջին գլուխը պարունակում է աշխատության մեջ օգտագործվող հասկացությունների հիմնական սահմանումները, նկարագրությունները և նշանակումները: Կառուցված և այլընտրանքային ծրագրային համալիրներում գործածվող կամ վերլուծության համար անհրաժեշտ գաղտնագրության գործիքների նկարագրությունները և կիրառական նշանակությունները, սիմետրիկ և ոչ սիմետրիկ բանալիով գաղտնագրման մեթոդները ևս բերված են այս գլխում: Ներկայացված են անվտանգ հաշվարկների խնդիրը, լուծումների հիմքում ընկած հիմնական հաղորդակարգերը և այլ բաղադրիչները: Քննարկված և վերլուծված են երկու մասնակցով և բազմամասնակից հաշվարկների իրականացման խնդիրները, դիտարկված են տարբերությունները: Նկարագրված են ֆունկցիաների տարբեր ներկայացումներ, մասնավորապես բուլյան և թվաբանական սխեմաների տեսքով ներկայացման մասին, որոնք օգտագործվում են անվտանգ հաշվարկների հաղորդակարգերում և ներկայացված են սպիտակ արկղի գաղտնագրության մեթոդները:

Աշխատության երկրորդ գլուխը նվիրված է սպիտակ արկղի անտեղյակ փոխանցումը ընդլայնող հաղորդակարգի կառուցմանը, որը թույլ է տալիս կտրուկ նվազեցնել անհրաժեշտ փոխանցումների քանակը: Նկարագրված են անտեղյակ փոխանցում իրականացնող տարբեր հաղորդակարգեր, վերլուծված են նրանց տարբերությունները հիմքում ընկած հասկացությունների, ալգորիթմական կառուցվածքի և անվտանգության ապահովման մակարդակի տեսանկյուններից: Բերված է անտեղյակ փոխանցման հաղորդակարգերի ընդլայնման գաղափարը և կառուցված է ընդլայնում սպիտակ արկղի անտեղյակ փոխանցման հաղորդակարգի համար:
Անտեղյակ փոխանցումը երկու մասնակցով գաղտնագրային հաղորդակարգ է, որը թույլ է տալիս կողմերից մեկին (ուղարկող) փոխանցել իր գաղտնիք հանդիսացող տվյալների մի մասը մյուս (ստացող) կողմին: Փոխանցման արդյունքում ստացող կողմը չի ստանում հաղորդակարգով նախատեսվածից բացի այլ տեղեկություններ ուղարկողի գաղտնիքների մասին, իսկ ուղարկող կողմը մնում է անտեղյակ, թե իր տվյալների որ մասը ստացավ մյուս կողմը :

Երկրորդ գլխի առաջին մասում նկարագրվում են անտեղյակ փոխանցման մի քանի հաղորդակարգեր, այդ թվում Ռաբինի ներմուծած տարբերակը, 1-ը 2-ից անտեղյակ փոխանցման հաղորդակարգը և դրա վերափոխված տարբերակը ստացողի համար ընտրման հնարավորությամբ, ինչպես նաև վերջինիս ընդհանրացում հանդիսացող 1-ը n-ից հաղորդակարգը: Ներկայացված հաղորդակարգերի տարբեր իրականացումներ վերլուծվում են արդյունավետության և անվտանգության տեսանկյուններից:
Ռաբինի ներմուծած սկզբնական տարբերակում ուղարկող կողմի մուտքային տվյալները p և q պարզ թվերն են, իսկ ստացող կողմը մուտք չունի: Ուղարկողը փոխանցում է այդ պարզ թվերի արտադրյալը ստացողին և վերջինս, հաղորդակարգի իրականացման արդյունքում $\frac{1}{2}$ հավանականությամբ դուրս է բերում այդ թվերը, իսկ ուղարկողը չի տեղեկանում արդյոք ստացողին հաջողվեց թվերի դուրսբերումը: 1-ը 2-ից անտեղյակ փոխանցման հաղորդակարգի դեպքում ուղարկող կողմի մուտքային տվյալները m_0 և m_1 գաղտնի հաղորդագրություններն են, իսկ ստացողինը՝ $\sigma \in \{0,1\}$ ընտրության բիթը: Հաղորդակարգի իրականացման արդյունքում ստացողը դուրս է բերում m_σ-ն և ոչինչ $m_{1-\sigma}$-ի մասին, իսկ ուղարկողը մնում է անտեղյակ σ-ի արժեքից: 1-ը n-ից անտեղյակ փոխանցումը 1-ը 2-ից հաղորդակարգի ընդհանրացումն է, որտեղ ուղարկողն ունի $m_1,\ldots, m_n$ գաղտնիքներ, իսկ ստացողը՝ $1 \le \sigma \le n$ ընտրության ցուցիչ: Հաղորդակարգի իրականացման արդյունքում ստացողը դուրս է բերում m_σ-ն և ոչ մի տեղեկություն մնացյալ գաղտնիքների մասին, իսկ ուղարկողը կրկին մնում է անտեղյակ σ-ի արժեքից:

Երկրորդ գլխի երկրորդ մասում ներկայացվում են սպիտակ արկղի գաղտնագրության մեթոդների հիմքի վրա կառուցված անտեղյակ փոխանցման հաղորդակարգերը և

դրանց համեմատական վերլուծությունները այլընտրանքային տարբերակների հանդեպ: Ներկայացված են երկու սպիտակ արկղի անտեղյակ փոխանցման հաղորդակարգ, որոնք իրականացնում են վերը սահմանված 1-ը 2-ից և 1-ը n-ից տարբերակները: Այս հաղորդակարգերի գլխավոր առավելությունը կայանում է նրանում, որ այլընտրանքներում օգտագործվող բաց բանալիով գաղտնագրման գործողությունների փոխարեն օգտագործվում են սպիտակ արկղի և սիմետրիկ գաղտնագրության հաշվարկային տեսանկյունից զգալիորեն արագ գործողությունները: Հաղորդակարգում ուղարկող հանդիսացող կողմը նախապես կառուցում է նախընտրելի սիմետրիկ գաղտնագրող մեթոդի սպիտակ արկղի ներկայացումը իր գաղտնի բանալու գործածմամբ և այն հասանելի դարձնում ստացող կողմին: Ստացողի գաղտնագրած հաղորդագրությունները ուղարկողը կարողանում է վերծանել՝ օգտագործելով գաղտնի բանալին: Ապացուցված է այս հաղորդակարգերի ապահով լինելը կիսաազնիվ (semi-honest) հակառակորդների (հակառակորդը հավաքում և վերլուծում է հաղորդակարգի իրականացման ընթացքում ստացված միջանկյալ հաղորդագրությունները, սակայն շարունակում է հետևել հաղորդակարգի քայլերին) գրոհների հանդեպ:
Երկրորդ գլխի երրորդ մասում ներկայացվում է կառուցված ընդլայնող հաղորդակարգը սպիտակ արկղի անտեղյակ փոխանցման հաղորդակարգի համար:

Մուտքային տվյալներ: S: l-բիթ երկարությամբ վեկտորների m զույգ $(x_j^0, x_j^1), x_j^1 \in \{0,1\}^l$.
R: m երկարությամբ ընտրության վեկտոր $r = (r_0, r_1, \dots, r_{m-1})$, $r_i \in \{0,1\}$, $0 \le i < m$.

Ընդհանուր մուտք: իրականացվելիք անտեղյակ փոխանցումների քանակ k,
ՍԱԱՓ – նախապես համաձայնեցված սպիտակ արկղի անտեղյակ փոխանցում

Քայլ 1: S-ը կառուցում է k երկարությամբ պատահական վեկտոր s,
R-ը կառուցում է $m \times k$-չափանի մատրից T՝ պատահական էլեմենտներով.

Քայլ 2: *ՍԱԱՓ* հաղորդակարգի իրագործում , որտեղ R-ը հանդիսանում է ուղարկող կողմ՝
$(t^i, t^i \oplus r)$; $0 \le i < k$ մուտքերով, իսկ S-ը՝ ստացող կողմ՝ s մուտքով:
S-ի ստացած վեկտոր-սյուները նշանակենք q^j-ով, նրանցով կազմված մատրիցը՝ Q-ով.

Քայլ 3: S-ն ուղարկում է R-ին l-երկարությամբ վեկտորների m զույգեր (y_j^0, y_j^1) , որտեղ $y_j^0 = x_j^0 \oplus H(j, q_j)$ և $y_j^1 = x_j^1 \oplus H(j, q_j + s)$, q_j-ն S-ից Քայլ 2-ում ստացված Q մատրիցի j-րդ տողն է.

R-ը ստանում է $x_j^{r_j} = y_j^{r_j} \oplus H(j, t_j)$, $0 \le j < m$.

Նկար 1: Սպիտակ արկղի անտեղյակ փոխանցման ընդլայնում $k \times \text{ՍԱԱՓ}_l \to m \times \text{ՍԱԱՓ}_l$

l երկարությամբ վեկտորների m հատ 1-ը n-ից անտեղյակ փոխանցումը, նշանակվում է $m \times OT_l$, սահմանվում է հետևյալ կերպ. S ուղարկող կողմը ունի l երկարությամբ $\{x_j^0, x_j^1\}$, $0 \le j < m$ վեկտորների m զույգ. R ստացող կողմը ունի m հատ ընտրության բիթ $r_0, r_1, \ldots, r_{m-1}$. Հաղորդակարգի իրականացումից հետո R-ը պետք է ունենա m հատ $\{x_j^{r_j}\}, 0 \le j < m$ վեկտորները, անտեղյակ մնալով S-ի մյուս վեկտորներից, իսկ S-ը անտեղյակ է մնում ընտրության բիթերից: Բիվերը ցույց է տվել, որ $m \times OT_l$ ֆունկցիոնալությունը կարելի է իրականացնել m-ից քիչ անտեղյակ փոխանցումներ իրականացնելով. Իշայի և այլոց՝ այս տեսական արդյունքին հաջորդած աշխատանքում կառուցվել է ընդլայնում, որում փոխանցումների քանակը նվազեցվել է մինչև k ֆիքսված թիվը: Այս բաժնում ներկայացվում են կառուցված երկու ընդլայնումները, որոնք սպիտակ արկղի անտեղյակ փոխանցման (ՍԱԱՓ) համար իրականացնում են $m \times ՍԱԱՓ_l$ ֆունկցիոնալությունը օգտագործելով $k \times ՍԱԱՓ_l$ (տես **Նկար 1**) և $k \times ՍԱԱՓ_k$ (տես **Նկար 2**) ֆունկցիոնալությունները:

Մուտքային տվյալներ: S: l-բիթ երկարությամբ վեկտորների m զույգ $(x_j^0, x_j^1), x_j^1 \in \{0,1\}^l$.
R: m երկարությամբ ընտրության վեկտոր $r = (r_0, r_1, \ldots, r_{m-1})$, $r_i \in \{0,1\}$, $0 \le i < m$.

Ընդհանուր մուտք: իրականացվելիք անտեղյակ փոխանցումների քանակ k,
ՍԱԱՓ – նախապես համաձայնեցված սպիտակ արկղի անտեղյակ փոխանցում

Քայլ 1: S-ը կառուցում է k երկարությամբ պատահական վեկտոր s,
R-ը կառուցում է k երկարությամբ պատահական վեկտորների k զույգ $\{k_i^0, k_i^1\}$, $0 \le i < k$.
$ՍԱԱՓ$ հաղորդակարգի իրագործում , որտեղ R-ը հանդիսանում է ուղարկող կողմ՝ $\{k_i^0, k_i^1\}, 0 \le i < k$ մուտքերով, իսկ S-ը՝ ստացող կողմ՝ s մուտքով:

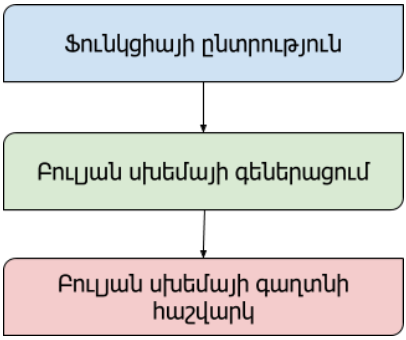
Քայլ 2: Կառուցվում է $m \times k$ չափերի T մատրից, որտեղ սյուները $t^i = G(k_i^0)$
R-ն ուղարկում է $u^i = t^i \oplus G(k_i^1) \oplus r, 0 \le i < k$ հաղորդագրություններ S-ին,
S-ը կառուցում է $m \times k$ չափերի Q մատրից, որի սյուներն են
$q^i = s_i * u^i \oplus G(k_i^{s_i})$, $0 \le i < k$

Քայլ 3: S-ն ուղարկում է R-ին k երկարությամբ (y_j^0, y_j^1) վեկտորների m զույգեր, որտեղ $y_j^0 = x_j^0 \oplus H(j, q_j)$ և $y_j^1 = x_j^1 \oplus H(j, q_j + s)$, որտեղ q_j-ն Քայլ 2-ում կառուցված Q մատրիցի j-րդ տողն է.

R-ը ստանում է $x_j^{r_j} = y_j^{r_j} \oplus H(j, t_j)$, $0 \le j < m$.

Նկար 2: Սպիտակ արկղի անտեղյակ փոխանցման ընդլայնում $k \times ՍԱԱՓ_k \to m \times ՍԱԱՓ_l$

Աշխատության երրորդ գլուխը նվիրված է կառուցված ԱԲՀ իրականացնող ծրագրային համալիրին: Այստեղ առկա է համալիրի ընդհանուր նկարագրությունը, համեմատումն այլ իրականացումների հետ, վերլուծությունն ու փորձնական տվյալները: Ներկայացված են համալիրի կառուցամասերը, աշխատանքի փուլերը և հիմքում ընկած GMW ԱԲՀ հաղորդակարգը: Այս գլխում նաև նկարագրվում է համալիրում ընդգրկված կոմպիլյատորը, որը նպատակային ֆունկցիայի բարձր մակարդակի ծրագրավորման լեզվով նկարագրության հիման վրա կառուցում է բուլյան սխեմա, որն անհրաժեշտ է GMW հաղորդակարգի աշխատանքի համար: Համալիրի աշխատանքի փուլերի ընդհանուր պատկերը զետեղված է Նկար 3-ում: Գլխի վերջում ներկայացվում է վերոնշյալ հաղորդակարգի փոփոխված տարբերակը, որում հնարավոր է ներառել հաշվարկման գործընթացին չմասնակցող, սակայն մուտքային և ելքային տվյալներ ունեցող կողմերի:

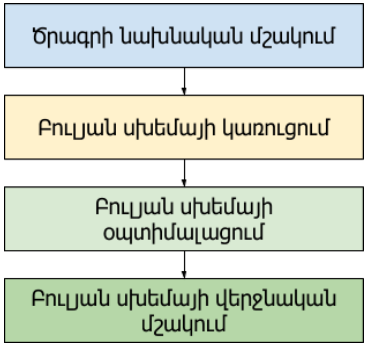


Նկար 3: ԱԲՀ համակարգի աշխատանքի ընդհանուր պատկերը

Երրորդ գլխի առաջին մասում ներկայացված են ԱԲՀ իրականացնող տարբեր համակարգեր, նրանց կիրառությունների ոլորտներն ու յուրահատկությունները: Մատնանշված են այդ համակարգերի թերությունները, որոնք առկա չեն մեր համակարգում: ShareMind ծրագրային համալիրը նախատեսված է միայն երեք մասնակիցներով հաշվարկների համար, ուստի զգալիորեն նեղացնում է իր կիրառույթունների տիրույթը՝ սահմանափակելով հաշվարկի մասնակիցների քանակը: VIFF և SEPIA համակարգերը հաշվարկները իրականացնում են թվաբանական սխեմաներով և հիմնված են հոմոմորֆ գաղտնագրության մեթոդների վրա, ինչը թույլ չի տալիս լավարկել այդ համակարգերը օգտագործելով անտեղյակ փոխանցման բարելավված մեթոդները: Այս համակարգերի անվտանգության պայմանները ևս տարբերվում են մեր իրականացրածից: GMW հաղորդակարգի հիման վրա Չոիի և այլոց իրականացումը համընկնում է մեր հետազոտության առարկայի հետ, սակայն

զգալիորեն զիջում է վերջինիս, բաց բանալիով գաղտնագրության մեթոդների գործածման պատճառով: Այստեղ նաև բացակայում է բուլյան սխեմա կառուցող կոմպիլյատոր, ինչը օգտագործողների տեսանկյունից լրացուցիչ դժվարություն է առաջացնում, քանի որ նրանք ստիպված են լինում ինքնուրույն կառուցել իրենց հետաքրքրող ֆունկցիաների համապատասխան սխեմաները:

Երրորդ գլխի երկրորդ մասում նկարագրվում է մեր համակարգում ընգրկված բարձր մակարդակի ծրագրավորման լեզվով ֆունկցիայի նկարագրությունից բուլյան սխեմաներ կառուցող կոմպիլյատորը: Այս բաղադրիչի առկայությունը հնարավորություն է ընձեռնում բուլյան սխեմաների սինթեզմանը անտեղյակ տարբեր ոլորտների մասնագետներին օգտագործել համակարգը՝ նպատակային ֆունկցիան նկարագրելով բարձր մակարդակի ծրագրավորման լեզվով, որի նկարագրությունը ևս բերված է այս բաժնում: Բերված են նաև կոմպիլյատորի իրականացման ընթացքում օգտագործված ծրագրային համակարգերի և գրադարանների, ինչպես նաև բուլյան սխեմայի կառուցման և լավարկման մեթոդների հակիրճ նկարագրությունը: Կոմպիլյատորի աշխատանքի փուլերը պատկերված են Նկար 4-ում:

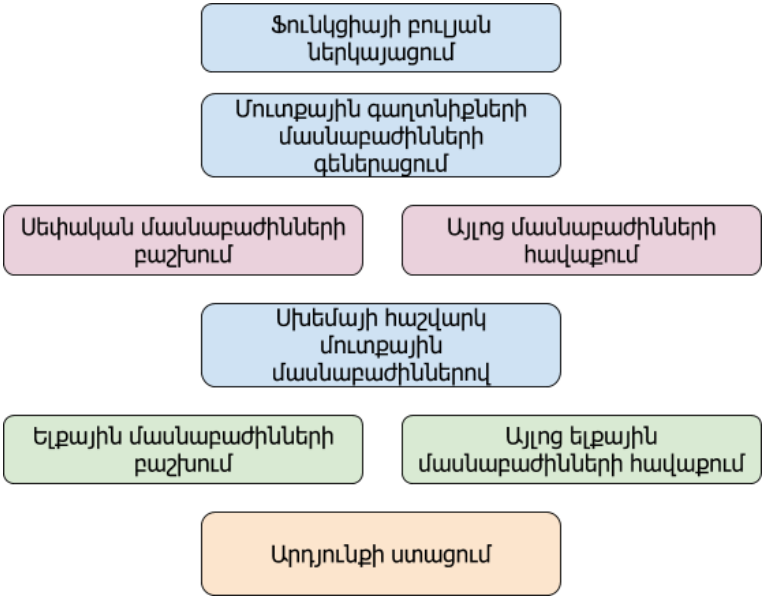


Նկար 4: Կոմպիլյատորի աշխատանքի հիմնական փուլերը

Ծրագրի նախնական մշակման փուլում կատարվում են մուտքային ծրագրի նկարագրության ձևափոխություններ հետագա փուլերի աշխատանքի համար: Բուլյան սխեմայի կառուցման փուլում ֆունկցիայի ձևափոխված նկարագրության հիման վրա տեղի է ունենում ըստ մոդուլ երկուսի գումարման և բազմապատկման հանգույցներով նախնական սխեմայի կառուցումը: Այստեղ կիրառվում են որոշ գործողությունների համար օգտագործվում են հատուկ ներկայացումներ, որոնք ավելի նախընտրելի են GMW հաղորդակարգի յուրահատկությունների տեսանկյունից: Մասնավորապես օգտագործվում են փոքր խորությամբ ենթասխեմաներ, որպեսզի փոքրացնեն հաղորդակարգի աշխատաժամանակը: Հաջորդ փուլում կառուցված սխեմայից

հեռացվում են կրկնվող և հաստատուն հանգույցները, ինչպես նաև սխեմայի ելքի վրա ազդեցություն չունեցող հանգույցները: Բուլյան սխեմայի վերջնական մշակման փուլում փոփոխությունների է ենթարկվում ելքային ֆայլի կառուցվածքը, որը թույլ է տալիս հեշտությամբ ստանալ սխեմայում միևնույն մակարդակում գտնվող բազմապատկող հանգույցները և նրանց հաշվարկման ընթացքում կատարել զուգահեռ անտեղյակ փոխանցումներ:

Երրորդ գլխի երրորդ մասը ներկայացնում է բուլյան սխեմայի հաշվարկման իրականացման գործընթացը: Այստեղ բերվում է GMW հաղորդակարգի նկարագրությունը, գաղտնիքների մասնատման սկզբունքը և հիմնավորումը և սխեմայի գործողությունների մասնաբաժիններով հաշվարկման մեթոդները: Նկար 5-ում պատկերված է անվտանգ հաշվարկման հաղորդակարգի ընթացքը օգտագործողի տեսանկյունից:



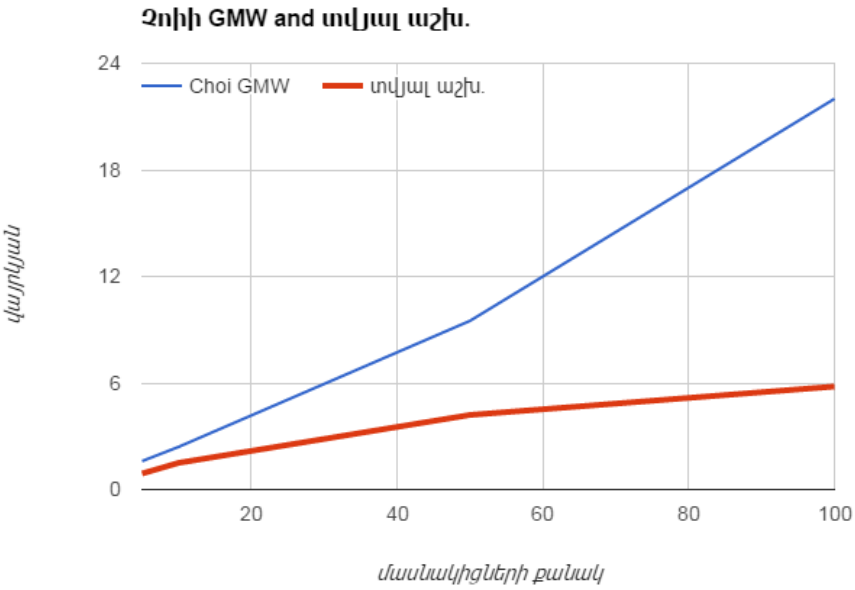
Նկար 5: ԱԲՀ հաղորդակարգի փուլերը հաշվարկին մասնակցող կողմի տեսանկյունից

Նպատակային ֆունկցիան որոշելուց և համակարգի կոմպիլյատորի միջոցով դրա համապատասխան բուլյան սխեման ստանալուց հետո մասնակիցները գործում են հետևյալ կերպ: Բոլոր կողմերը իրենց մուտքային տվյալների համար գեներացնում են գաղտնի մասնաբաժիններ և յուրաքանչյուր մասնակցին տալիս մի մասը: $P_1, \dots, P_n$ մասնակիցներ ենթադրող հաշվարկի գործընթացում յուրաքանչյուր կողմ բուլյան

սխեմայում իր մուտքերին համապատասխանող յուրաքանչյուր w լարի համար պատահականորեն գեներացնում է $n-1$ մասնաբաժին և ընտրում n-րդ այնպես, որ $\oplus_{i=1}^{n} s_{wi} = s_w$, որտեղ $s_w \in \{0,1\}$ w լարի մուտքային արժեքն է, $s_{wi} \in \{0,1\}, 1 \leq i \leq n$ P_i մասնակցի մասնաբաժինն է այդ լարի արժեքից: Այսպիսով, լարի իրական արժեքը գտնելու համար գրոհողը պետք է պարզի բոլոր մասնաբաժինները, այսինքն պետք է գրոհի կամ ղեկավարի բոլոր մասնակիցներին: Ստացվում է, որ մասնակցի մուտքային տվյալները սկզբնական փուլում առանց մասնակցին գրոհելու չի կարելի պարզել, նույնիսկ ղեկավարել մյուս բոլոր կողմերին:

Երբ բոլոր մուտքային լարերի արժեքների մասնատումը և բաշխումը կատարված է, յուրաքանչյուր մասնակից ունի բուլյան սխեմա, որոշակի մուտքային արժեքներով: Հաջորդ փուլում կողմերը սկսում են հաշվարկել սխեման տեղային կամ այլոց հետ հաղորդակցությունների միջոցով, երբ պահանջվում է, քանի որ ընթացող հաշվարկի ավարտից հետո կողմերը ցանկանում են վերականգնել վերջնական արդյունքը դրա մասնաբաժիններից: Այս պայմանի բավարարման համար հանգույցների հաշվարկը կատարվում է հետևյալ կերպ. XOR հանգույցների հաշվարկումը անցկացվում է տեղային և որպես հանգույցի ելքային արժեք ընտրվում է մուտքային մասնաբաժինների գումարը ըստ մոդուլ երկուսի: AND հանգույցների հաշվարկը ավելի բարդ գործընթաց է և պահանջում է հաղորդակցություն իրականացնել այլ մասնակիցների հետ: Մեկ AND հանգույցի հաշվարկման համար անհրաժեշտ է կատարել $\binom{n}{2}$ 1-ը 4-ից անտեղյակ փոխանցում, որոնցից յուրաքանչյուրը կարելի է իրականացնել երկու 1-ը 2-ից անտեղյակ փոխանցման միջոցով: Այս հանգույցների հաշվարկման գործընթացը մանրամասնորեն ներկայացված աշխատության համապատասխան բաժնում:

GMW հաղորդակարգի արագագործությունը մեծապես կախված է AND հանգույցների հաշվարկման արագությունից և հետևաբար անտեղյակ փոխանցումների իրականացման արագությունից: Այս աշխատությանը նախորդող իրականացումներում օգտագործում էին բաց բանալիով գաղտնագրության գործողություններ, որոնց հաշվարկումը ժամանակատար է: Ներկայացնելով սպիտակ արկղի անտեղյակ փոխանցման առաջին կիրառումը նման հաղորդակարգերում, այս աշխատանքը զգալիորեն բարելավում է նախկին իրականացումների արագագործության ցուցանիշները: Չոիի և այլոց աշխատանքի և տվյալ աշխատանքի միջև անցկացված արագագործությունների համեմատության արդյունքները պատկերված են Նկար 6-ում: Արդյունքների էապես բարելավվումը հիմնականում պայմանավորված է բաց բանալիով գաղտնագրային գործողություններից խուսափելով և երկրորդ գլխում ներմուծված ՍԱԱՓ ընդլայնման հաղորդակարգի օգտագործմամբ:



Նկար 6: Չոիի և տվյալ աշխատանքում ներկայացվող GMW հաղորդակարգի իրականացումների համեմատություն

Երրորդ գլխի չորրորդ մասում ներկայացվում է GMW հաղորդակարգի ընդլայնում, որը բացի դասական մասնակիցներից (ակտիվ մասնակիցներ) թույլ է տալիս հաշվարկման տեսանկյունից այսպես կոչված պասիվ կողմերի մասնակցություն: Պասիվ մասնակիցները, ինչպես և ակտիվ մասնակիցները, ունեն գաղտնի մուտքային տվյալներ հաշվարկվող ֆունկցիայի համար և ելքային տվյալներ նույնպես, սակայն չեն մասնակցում բուլյան սխեմաների հաշվարկման գործընթացներին: Այսպիսի մասնակիցներին ներգրավելը իմաստալից է, երբ խոսքը գնում է թույլ հաշվողական և ցանցային հաղորդակցության սահմանափակ հնարավորություններով կողմերին: Ընդհանուր դեպքում մասնակիցների քանակը $n+m$ է, որտեղ n-ը ակտիվ մասնակիցների քանակն է, իսկ m-ը պասիվներինը: ինչպես և հիմնական հաղորդակարգում, ակտիվ մասնակիցներից յուրաքանչյուրը գեներացնում է $n-1$ պատահական մասնաբաժիններ սխեմայում իր ունեցած ամեն մուտքային լարի համար և բաշխում դրանք ակտիվ մասնակիցների միջև, իսկ իր n-րդ մասնաբաժինը ընտրում է նույն եղանակով: Պասիվ մասնակիցներից յուրաքանչյուրը կրկնում են վերոնշյալ գործողությունները այն տարբերությամբ, որ ստացված n մասնաբաժինները բաշխում են բոլոր ակտիվ մասնակիցների միջև, չպահելով սեփական մասնաբաժին: Այս դեպքում առաջանում է պասիվ մասնակիցների մուտքային տվյալների խոցելիություն,

որը դրսևորվում է, երբ բոլոր ակտիվ մասնակիցները ղեկավարվում են գրոհողի կողմից: Այդ իսկ պատճառով այս հաղորդակարգը անվտանգության տեսանկյունից զիջում է GMW-ին՝ պահանջելով գոնե մեկ ակտիվ մասնակցի առկայություն, ով չի գտնվում գրոհողի ազդեցության ոլորտում:

Աշխատանքի հիմնական արդյունքները

- Նախագծվել և իրականացվել է անվտանգ բազմամասնակից հաշվարկների համակարգ, որն ունի բարելավված արագագործություն նախկին իրականացումների համեմատ:
- Կառուցվել է սպիտակ արկղով անտեղյակ փոխանցման հաղորդակարգի ընդլայնում, որը թույլ է տալիս նվազեցնել անհրաժեշտ անտեղյակ փոխանցումների քանակը:
- Իրականացվել է մուտքային ֆունկցիայի բարձր մակարդակի լեզվով նկարագրությունից բուլյան սխեմա կառուցող կոմպիլյատոր՝ հաշվի առնելով օգտագործվող ԱԲՀ հաղորդակարգի առանձնահատկությունները:

Ատենախոսության թեմայով տպագրված հոդվածները

[1] A. H. Jivanyan, G.H. Khachatryan, T. V. Sokhakyan and D. H. Danoyan. Acceleration of Secure Function Evaluation Protocol. Computer Science and Information Technologies (CSIT), 2015, pp 115-118.

[2] D. H. Danoyan and T. V. Sokhakyan. A Generic Framework for Secure Computations. Proceedings of the Russian-Armenian (Slavonic) University #2, Physical-Mathematical Sciences, 2015, pp. 14-21.

[3] D. H. Danoyan. Extending White-Box Cryptography Based Oblivious Transfer Protocol. Proceedings of the Yerevan State University #1 (239), Physical and Mathematical Sciences, 2016, pp. 40-44.

[4] D. H. Danoyan, "Secure Multiparty Computations for Collaboration Between Competing Service Providers", Transactions of IIAP of the NAS RA, Mathematical Problems of Computer Science, vol. 45, pp. 59-66, 2016.

ABSTRACT

Davit H. Danoyan

"Secure multiparty computations based on a novel oblivious transfer protocol"

Suppose mutually distrustful parties $P_1, \ldots, P_n$ are willing to cooperate for computation of a preliminarily determined function with their private inputs. The computation might not include any trusted parties and nothing should be revealed to any party or coalition of parties about someone's input beyond what could be implied from the function output itself. One of key properties of secure multiparty computation (SMC) is the elimination of trusted parties. Without these protocols computations are being conducted in a centralized manner. This approach, although being very effective with regards to performance, has several security threats which are irrelevant for SMC. First, the collection and/or processing of secrets by a central party enable adversaries to concentrate attacks on that party only. Second, there computations can possibly be conducted in areas where revealed secrets can cost human lives. In case of some computations carried out in military or intelligence services trusted parties are impermissible. Also medical records of patients are private and cannot be shared among hospitals or other organizations.

Research objectives.
The purpose of the thesis is to design and implement a generic framework for secure multiparty computation, construction of an extension protocol to white-box oblivious transfer protocol which will decrease the required invocation count of the latter, resulting in enhancement of the overall performance of the applications based on the framework and design of applications using the framework's capabilities. The lifecycle of implemented framework consists of the following stages:

- The participants of computation input a program implementing their desired function described in a high level programming language.
- A single pass Boolean circuit implementing the same function is being generated by the compiler module of the framework.
- The generated circuit is being executed securely based on GMW SMC protocol.

Practical significance of results.
The results are important for the following scenarios of practical interest:

- The framework consists of separate modules, which allows to integrate or replace those with new developments in the field, resulting in enhancement of overall performance.

- The framework can be used for implementing secure voting and rating systems, as well as for research in bioengineering.
- The proposed extension for GMW protocol adds computationally passive parties.

Scientific novelty.

Design and implementation of a generic framework for secure multiparty computations, which:

- use of white-box cryptography based oblivious transfer instead of public-key methods in field of SMC,
- construction of an extension protocol to white-box oblivious transfer(WBOT) that reduces required WBOT invocation count,
- enables participation of computationally passive participants.

The main results of the thesis are:

- Design and implementation of secure multiparty computation framework with enhanced performance compared to existing implementations.
- Extension protocols for white-box oblivious transfer protocols.
- A generalization for GMW SMC protocol enabling participation of computationally passive participants.

РЕЗЮМЕ

Давид А. Даноян

«Безопасные многосторонние вычисления основанные на новом протоколе забывчивой передачи»

Предположим, что взаимно недоверчивые стороны $P_1, \ldots, P_n$ готовы сотрудничать для вычисления заведомо установленной функции с их частными конфиденциальными входными данными. Вычисление может не включать в себя каких-либо доверенных сторон и ничто не должно быть раскрыто о частных входах, кроме того, что могло бы вытекать из значения самой функции, для какой-либо стороны или коалиции сторон.
Одним из ключевых свойств безопасного многостороннего вычисления (БМВ) является устранение доверенных сторон. Без этих протоколов, вычисления проводятся централизованно. Такой подход, хотя и является очень эффективным в отношении производительности, имеет несколько угроз безопасности, которые отсутствуют в БМВ. Во-первых, сбор и/или обработка секретов центральной стороной позволяют злоумышленников сосредоточить атаки только на этой стороне. Во-вторых, вычисления могут проводиться в областях, где раскрытия тайн могут стоить человеческих жизней. В случае некоторых вычислений, проведенных в военных или разведывательных службах, доверенные стороны недопустимы. Также, медицинские записи пациентов конфиденциальны и не могут быть переданы между больницами или другими организациями.

Цели работы.

Цель диссертации заключается в разработке и реализации общей основы для безопасного многостороннего вычисления, построение расширенного протокола забывчивой передачи белого ящика, который позволит уменьшить требуемое количество вызова последнего, что приводит к повышению эффективности работы приложений, основанных на платформе и дизайне приложений, использующих возможности фреймворка. Жизненный цикл реализованной основы состоит из следующих этапов:

- Стороны вычислений вводят программу, реализующую их желаемую функцию - описанную на языке программирования высокого уровня.
- Модулем компилятора платформы генерируется однопроходная булева схема реализации той же функции.
- Сгенерированная схема выполняется безопасно за счет протокола GMW БМВ с выбранными оптимизациями.

Практическая ценность.

Результаты имеют важное значение для следующих сценариев, представляющих практический интерес:

- Платформа состоит из отдельных модулей, что позволяет интегрировать новые разработки в этой области или заменить ими имеющиеся, что приводит к повышению общей производительности.
- Платформа может быть использована для реализации безопасного голосования и рейтинговых систем, а также для исследований в области биоинженерии и анализа данных.
- Предлагаемое расширение для протокола GMW добавляет пассивные в вычислительном отношении стороны.

Научная новизна.

Разработка и реализация общей платформы для безопасных многосторонних вычислений, которая:

- использует забывчивую передачу основанную на криптографии белого ящика вместо методов, основанных на шифровании с открытым ключом,
- использует новый протокол расширения для белого ящика забывчивой передачи, чтобы уменьшить количество вызова забывчивой передачи,
- дает возможность участия пассивных в вычислительном отношении участников.

Основные результаты диссертационной работы:

- Разработана и реализована платформа для безопасных многосторонних вычислений с повышенной производительностью по сравнению с существующими реализациями.
- Построено расширение для протокола забывчивой передачи основанного на криптографии белого ящика, сокращающий количество выполнений протокола.
- Разработан компилятор использующий особенности безопасных многосторонних вычислений, который генерирует булеву схему реализующую функцию написанную на языке высокого уровня.