ՀՀ ԳԱԱ ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ
ԻՆՍՏԻՏՈՒՏ

Ջիվանյան Արամ Հարությունի

Էլեկտրոնային քվեարկության նոր համակարգերի մշակում և իրականացում

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

Սեղմագիր

Երևան – 2013

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И
АВТОМАТИЗАЦИИ НАН РА

Дживанян Арам Арутюнович

Разработка и реализация новых систем электронных голосований

Автореферат

диссертации на соискание ученой степени кандидата
технических наук по специальности
05.13.05 – “Математическое моделирование, численные методы и
комплексы программ”

Ереван – 2013

Ատենախոսության թեման հաստատվել է Հայ-Ռուսական (Սլավոնական) համալսարանում:

Գիտական ղեկավար՝ տ.գ.դ. Գ.Հ. Խաչատրյան

Պաշտոնական ընդդիմախոսներ՝ ֆ.մ.գ.դ. Լ.Ասլանյան
տ.գ.թ. Ռ. Բարսեղյան

Առաջատար կազմակերպություն՝ Երևանի պետական համալսարան

Պաշտպանությունը կայանալու է 2013թ.-ի մայիսի 14-ին, ժամը 15:00-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում հետևյալ հասցեով՝ 0014, Երևան, Պ.Սևակի 1:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ԳԱԱ ԻԱՊԻ-ի գրադարանում:

Սեղմագիրն առաքված է 2013թ.-ի ապրիլի 13-ին:

037 մասնագիտական խորհրդի
գիտական քարտուղար, ֆ.մ.գ.դ. Հ.Գ. Սարուխանյան

Тема диссертации утверждена в Российско-Армянском (Славянском) Университете

Научный руководитель: д.т.н. Г.А. Хачатрян

Официальные оппоненты: д.ф.м.н. Л.Асланян
к.т.н. Р. Барсегян

Ведущая организация: Ереванский государственный университет

Защита состоится 14-го мая 2013г. в 15:00 на заседании специализированного совета 037 "Информатика и вычислительные системы" Института проблем информатики и автоматизации НАН РА по адресу: 0014, Ереван, ул. П. Севака, 1.

С диссертацией можно ознакомиться в библиотеке ИПИА НАН РА.

Автореферат разослан 13-го апреля 2013г.

Ученый секретарь специализированного
совета 037, д.ф.м.н. А.Г. Саруханян

Աշխատանքի ընդհանուր բնութագիրը

Թեմայի արդիականությունը

ԱՄՆ-ի նախագահական ընտրությունների ժամանակ 2000թ-ին կիրառվեցին Էլեկտրոնային քվեարկության հատուկ սարքեր(DRE մեքենաներ), որոնք ստեղծված էին հեշտացնելու քվեարկության պրոցեսը և ապահովելու ձայների արագ, ճշգրիտ հաշվարկ: Սակայն ընտրությունների ընթացքում գրանցվեցին բազմաթիվ թերություններ, ինչից հետո քվեարկության այդ համակարգերի հանդեպ վստահությունը կասկածի տակ դրվեց: ԱՄՆ առաջատար համալսարաններից երկուսի՝ Կալիֆոռնիայի Տեխնոլոգիական համալսարանի(CalTech) և Մասաչուսեթսի Տեխնոլոգիական համալսարանի(MIT) նախաձեռնությամբ հիմք դրվեց մի գիտահետազոտական նախագծի, որի նպատակն էր վերլուծել օգտագործված DRE մեքենաների անվտանգության բոլոր հատկանիշները, քվեների կեղծման կամ չգրանցման բոլոր հնարավորությունները, ինչպես նաև քվեարկությունները էլեկտրոնային եղանակով անցկացնելու հեռանկարները: Արդյունքում հայտնաբերվեց, որ գոյություն ունեցող բոլոր էլեկտրոնային քվեարկության մեքենաները լայն հնարավորություն են տալիս տարբեր տիպի չարագործներին (չարագործ կարող է հանդիսանալ ծրագրային կոդը, ծրագրին միջամտող ինֆորմացիոն չարագործները, տվյալների պահոցի ադմինիստրատորները և այլն) փոխել գրանցված քվեները, մերժել ընտրողի քվեները և չգրանցել քվեաթերթիկները, կամ գրանցել հիսուն հազար քվե մի ընտրատեղամասում, որտեղ իրավասու ընտրողների թիվը հազար է: Եզրակացությունը մեկն էր՝ ընտրությունները դեռևս չի կարելի անցկացնել էլեկտրոնային եղանակով, քանի որ գոյություն ունեցող համակարգերը չեն բավարարում անհրաժեշտ անվտանգության հատկանիշներին: Այս հանգամանքը հիմք հանդիսացավ վերադառնալու J. Cohen-ի և M. J. Fischer-ի կողմից 1985թ-ին առաջարկված կրիպտոգրաֆիկ Էլեկտրոնային քվեարկության տեսական ալգորիթմին, որը ընտրողին հնարավորություն էր տալիս հետևել իր քվեի ճիշտ գրանցմանը և հաշվարկին՝ միաժամանակ չբացահայտելով քվեի գաղտնիությունը: Ընտրություններում քվեների միաժամանակ վերահսկելիություն և գաղտնիություն ապահովելու հնարավորությունը առաջին անգամ ցույց է տրվել 1980թ-ի Chaum-ի կողմից: Նման համակարգերի նախագծման հիմքում ընկած է այն դատողությունը, որ էլեկտրոնային քվեարկությունների անվտանգությունը պետք է ապահովված լինի ոչ թե ֆիզիկական միջոցների՝ համակարգիչների կամ ծրագրային ապահովման անվտանգությամբ, այլ քվեարկության ընթացակարգի մաթեմատիկական հատկություններով: Այն պետք է թույլ տա բացահայտել քվեների հետ տեղի ունեցած ցանկացած կեղծիք կամ քվեների հաշվարկի հետ կապված ցանկացած անճշտություն: Այժմ գոյություն ունեն կրիպտոգրաֆիկ քվեարկության հարյուրավոր ընթացակարգեր, որոնք այս կամ այն չափով ապահովում են այդ երկու հիմնական հատկությունները՝ ընտրությունների վերահսկելիությունը և քվեների գաղտնիության պահպանումը: Այդ ընթացակարգերի մեծամասնությունը, Cohen-ի և M. J. Fischer-ի ընթացակարգի նմանությամբ, ընտրողից պահանջում է քվեարկության ընթացքում ինքնուրույն կատարել բարդ կրիպտոգրաֆիկ գործողություններ, ինչը համակարգը դարձնում է ոչ կիրառելի: Որոշ կրիպտոգրաֆիկ համակարգեր հիմնված են հատուկ թղթե քվեաթերթիկների վրա, ինչը համակարգը խոցելի է դարձնում մի շարք հարձակումների նկատմամբ, մասնավորապես, հնարավոր է դառնում շղթայական քվեարկությունների կազմակերպում: Նորվեգիայում 2011թ-ին կիրառվեց էլեկտրոնա-

յին քվեարկության համակարգ, որը ընձեռում էր քվեների գրանցման և ձայների հաշվարկի բացարձակ վերահսկելիության մեխանիզմ, սակայն ընտրողին տրամադրված անդորրագրերի շնորհիվ թույլ էր տալիս բացահայտել ընտրողի քվեն: Էլեկտրոնային քվեարկության համակարգ կիրառվել է նաև Հայաստանում 2012թ-ին, որը սակայն չէր ապահովում ընտրությունների վերահսկելիություն: Արդյունքում պարզ է դառնում նոր կրիպտոգրաֆիկ էլեկտրոնային քվեարկության համակարգի մշակման անհրաժեշտությունը, որը հնարավորություն կտա վերահսկելիություն սահմանել ընտրողի քվեի գրանցման, չփոփոխման և ճշգրիտ հաշվարկի վրա: Համակարգը պետք է ապահովի քվեի գաղտնիությունը ընտրությունների ողջ ընթացքում և հետո, այն չպետք է հիմնված լինի թղթե քվեաթերթիկների վրա և միաժամանակ պետք է կիրառելի լինի օգտագործողի տեսակետից:

Աշխատանքի նպատակը

Աշխատանքի նպատակն է մշակել այնպիսի էլեկտրոնային քվեարկության կրիպտոգրաֆիկ ընթացակարգ, որը հիմնված չէ թղթե քվեաթերթիկների վրա և

- ընձեռում է ընտրությունների ամբողջական վերահսկելիության մեխանիզմներ (universal verifiability).
- ապահովում է քվեների գաղտնիությունը ընտրական ողջ պրոցեսի ընթացքում և հետո(secrecy).
- արդյունավետ է արտադրողականության տեսակետից(efficiency).
- կիրառելի է օգտագործողի տեսակետից(usability).
- չի պահանջում հատուկ սարքեր, որոնք ավելացնում են ընտրությունների ծախսերը.

Հետազոտման մեթոդները

Աշխատանքում օգտագործված են բաց բանալով գաղտնագրության, 0-ինֆորմատիվ ապացույցների(zero-knowledge proofs), անանուն կապուտիների ստեղծման, կրիպտոգրաֆիկ ընթացակարգերի անվտանգության վերլուծության մեթոդները:

Արդյունքների գիտական նորությունը

- Մշակվել է էլեկտրոնային քվեարկության նոր ընդհանրացված ընթացակարգ, որն ապահովում է քվեների գաղտնիություն և ընտրությունների համընդհանուր վերահսկելիություն:
- Վերլուծվել է մշակված ընթացակարգի անվտանգության հատկանիշները:
- Ըստ մշակված ընդհանրացված ընթացակարգի առաջարկվել է էլեկտրոնային քվեարկության երկու նախատիպային մոտեցում: Առաջին մոտեցման հիմքում ընկած է ընտրողի կողմից քվեաթերթիկում թեկնածուների ցուցակը պատահական կերպով խառնելու մոտեցումը: Այս մոտեցման հիման վրա իրականացվել է SecureVoting քվեարկության ծրագրային համակարգը: Երկրորդ մոտեցման հիմքում ընկած է ընտրողի ներմուծած տրամաբանական վեկտորի օգնությամբ XOR գործողության միջոցով ընտրողի նշած թեկնածուի կողի գաղտնագրումը:

- Նշված ընթացակարգի համար առաջարկվել է հատուկ MIX ցանցի կառուցման նոր եղանակ և տրվել է MIX ցանցի գործունեության ստուգման ալգորիթմ:
- Վերլուծվել է 2011թ-ից Հայաստանում օգտագործվող էլեկտրոնային քվեարկության համակարգը և նկարագրվել է այդ համակարգում ձայների գաղտնիության և ընտրությունների ամբողջականության դեմ ուղղված մի շարք հնարավոր հարձակումներ: Առաջարկվել է նոր էլեկտրոնային քվեարկության ընթացակարգ, որն ապահովում է քվեների գաղտնիություն՝ միաժամանակ տրամադրելով քվեների՝ տվյալների բազայում ճիշտ գրանցման և ձայների հաշվարկի վերահսկելիություն:

Ստացված արդյունքների կիրառական նշանակությունը

Ատենախոսության շրջանակում մշակված էլեկտրոնային քվեարկության նոր ընթացակարգերը տեղ են գտել Հայաստանի Ամերիկյան Համալսարանում դասավանդվող «Կիրառական կրիպտոգրաֆիա» առարկայի դասախոսու- թյուններում: Մշակված ալգորիթմների հիման վրա կառուցվել է էլեկտրոնային քվեարկության SecureVoting համակարգը, որն առանց հատուկ տիպի մեխանիկական սարքեր պահանջելու թույլատրում է արդյունավետ կերպով իրականացնել վերահսկելի ընտրություններ:

Ներդրումներ

Աշխատանքում մշակված էլեկտրոնային քվեարկության ընթացակարգերը ներառվել են Հայաստանի ամերիկյան համալսարանում դասավանդվող «Կիրառական կրիպտոգրաֆիա» առարկայի դասընթացում: Ներդրման ակտը կցված է ատենախոսությանը:

Պաշտպանության են ներկայացվում հետևյալ դրույթները

- Նոր էլեկտրոնային քվեարկության ընթացակարգի մշակումը, որն ապահովում է քվեների գաղտնիություն՝ բաշխված գաղտնագրության համակարգերի և անանուն կապուղիների օգտագործման միջոցով: Ընթացակարգն ապահովում է նաև քվեների ճիշտ մուտքագրման, գրանցման և հաշվարկի բացարձակ վերահսկելիություն:
- Նոր MIX ցանցի կառուցումն առաջարկված ընթացակարգի համար, ինչպես նաև վերջինիս գործունեության ճշտության ստուգման ալգորիթմը:
- Հայկական էլեկտրոնային քվեարկության համակարգի վերլուծությունն ու էլեկտրոնային քվեարկության նոր ընթացակարգը:
- Առաջարկված էլեկտրոնային քվեարկության ընթացակարգի հիման վրա կառուցված էլեկտրոնային ընտրությունների կազմակերպման SecureVoting ծրագրային համակարգը:

Approbation and publications

Ատենախոսության հիմնական արդյունքներն ու դրույթները քննարկվել և զեկուցվել են ՀԱՀ «Computer and Information Science» հետազոտական կենտրոնի սեմինարների ընթացքում (2010-2013), «Applications of Information Theory, Coding and Security» գիտաժողովում (WAITC 2010., ք. Երևան), «Computer Science and Information

Technologies» միջազգային գիտաժողովում(CSIT 2011թ., ք. Երևան), Duisburg-Essen համալսարանի IEM գիտական սեմինարներում (2011թ., ք. Էսսեն, Գերմանիա), «Georgian ICT Development and Cyber Security Event» միջազգային գիտաժողովում(GITI 2012թ., ք. Թբիլիսի, Վրաստան), ՌՀՀ ՄԲՏԻ գիտական սեմինարում (2013թ., ք.Երևան, Հայաստան), ՀՀ ԳԱԱ ԻԱՊԻ գիտական սեմինարում (2013թ., ք. Երևան, Հայաստան):

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

Աշխատանքի կառուցվածքն ու ծավալը

Ատենախոսությունը բաղկացած է ներածությունից, չորս գլուխներից, եզրակացությունից և օգտագործված գրականության ցանկից: Աշխատանքի ընդհանուր ծավալն է 112 էջ, օգտագործված գրականության ցանկն ընդգրկում է 99 անուն:

Աշխատանքի բովանդակությունը

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

Առաջին գլխում դիտարկված են էլեկտրոնային քվեարկության համակարգերի առավելությունները դասական քվեարկության համակարգերի նկատմամբ: Ցույց է տրված, թե ինչպես կրիպտոգրաֆիայի կիրառությամբ կարելի է ընտրությունների ժամանակ ապահովել քվեների գաղտնիության պահպանում և միաժամանակ տրամադրել քվեի՝ համակարգչի կողմից ճիշտ մուտքագրման, տվյալների պահոցում ճիշտ գրանցման և քվեների ճշգրիտ հաշվարկի վերահսկելիության մեխանիզմներ: Վերահսկելիության մեխանիզմների առկայությունը նշանակում է, որ ընտրողը, քվեարկելով ոչ վստահելի էլեկտրոնային համակարգով, պետք է կարողանա ՝

1. Ստուգել և համոզվել, որ համակարգիչը չի կեղծել իր մուտքագրած քվեն, իսկ կեղծիքի առկայության դեպքում բացահայտել այն՝ ունենալով կեղծիքի առկայության հիմնավոր ապացույց:
2. Համոզվել, որ իր գրանցած քվեաթերթիկը, որը մինչև ձայների հաշվարկի փուլը պահվում է ոչ վստահելի տվյալների պահոցում, չի փոփոխվել չարագործների կողմից: Քվեաթերթիկի փոփոխված կամ ջնջված լինելու դեպքում ընտրողը պետք է կարողանա բացահայտել այդ կեղծիքը՝ ունենալով կեղծիքի առկայության հիմնավոր ապացույց:
3. Ստուգել, որ իր քվեն մասնակցում է ձայների հաշվարկին և ձայների հաշվարկի վերջում գրանցվում է հենց այն թեկնածուի օգտին, ում նախընտրել է ինքը՝ ընտրողը:

Վերահսկելիության այս երեք ստուգումները ապահովում են ընտրությունների համընդհանուր վերահսկելիության ամբողջական շղթան: Էլեկտրոնային քվեարկության համակարգը պետք է կարողանա ապահովել համընդհանուր վերահսկելիության ՝ միաժամանակ թույլ չտալով ընտրողի քվեի գաղտնիության բացահայտումը ընտրութ-

յունների ողջ ընթացքում կամ ընտրություններից հետո: Այդ պատճառով այս գլխում նաև մանրամասն ներկայացված և սահմանված են էլեկտրոնային քվեարկության համակարգերի անվտանգության հատկանիշների լայն սպեկտրը: Ցույց են տրված այդ հատկանիշները ապահովելու ժամանակ ի հայտ եկող բարդությունները:

Ներկայացված են կրիպտոգրաֆիկ քվեարկության համակարգերի ստեղծման գոյություն ունեցող հիմնական մոտեցումները: Դիտարկված են այդ տարբեր մոտեցումների առավելությունները և թերությունները: Բերված է էլեկտրոնային անվտանգ համակարգեր նախագծելու համար անհրաժեշտ մաթեմատիկական հենքը, օգտագործվող կրիպտոգրաֆիկ մեթոդների նկարագրությունը:

Գլխում վերլուծված են կրիպտոգրաֆիկ քվեարկության համակարգերի ստեղծման ասպարեզում կատարված հետազոտական աշխատանքները: Ավելի մանրամասն ներկայացված է արդի ամենազարգացած և արդեն իսկ կիրառված համակարգերի ֆունկցիոնալ նկարագրությունը, նրանց անվտանգության հատկանիշները:

Գլխի վերջում կատարված հետազոտությունների հիման վրա ձևավորվել է աշխատանքի նպատակը:

Երկրորդ գլխում ներկայացված է էլեկտրոնային քվեարկության նոր ընդհանրացված ընթացակարգ(e-voting protocol), որի հիման վրա կառուցած համակարգը հնարավորություն է տալիս իրականացնել համընդհանուր վերահսկելի ընտրություններ՝ միաժամանակ պահպանելով ընտրողների քվեների գաղտնիությունը ընտրական գործընթացի ողջ ընթացքում և հետո: Այդ ընդհանրացված ընթացակարգի հիման վրա առաջարկվել են քվեարկության երկու տարբեր մոտեցումներ: Առաջինը հիմնված է ընտրողի կողմից տրամաբանական վեկտոր-գաղտնիքների ներմուծման վրա, որոնցով XOR գործողության միջոցով գաղտնագրվում է ընտրողի քվեն: Երկրորդ մոտեցումը հիմնված է թեկնածուների ցուցակի վրա ընտրողի կողմից պատահական տեղափոխությունների կիրառման մեթոդի վրա:

Մեր առաջարկած էլեկտրոնային քվեարկության ընթացակարգը հիմնված է El-Gamal գաղտնագրության համակարգի վրա: Նշանակենք G-ով Z_P^*-վերջավոր դաշտի մուլտիպլիկատիվ խմբի Q կարգի ենթախումբը, որի ծնիչը g-ն է: Այստեղ P-ն և Q-ն մեծ (1024 բիթ կամ ավել) պարզ թվեր են, որտեղ $P = 2Q + 1$: Այսուհետ բոլոր գործողությունները տեղի են ունենում վերջավոր դաշտում, եթե հակառակը նշված չի: Ֆիքսենք $C = \{c_1, c_2, \dots, c_L\}$ բազմությունը, որտեղ L-ը ընտրությանը մասնակցող թեկնածուների քանակն է, իսկ c_i-ն՝ i-րդ թեկնածուի կոդը: $S = \{s_1, s_2, \dots, s_{|s|}\}$ բազմությամբ սահմանենք ընտրողի "գաղտնիքների" արժեքների տիրույթը, և $T = \{t_1, \dots, t_{|T|}\}$ բազմությամբ սահմանենք ընտրողին տրվող "անդորրագրային կոդերի" արժեքների բազմությունը: Ընթացակարգում օգտագործվում են այնպիսի $f: C \times S \to T$ ձևափոխություններ, որոնք բավարարում են հետևյալ երեք հատկություններին.

1. *Անհակադարձելիություն*: Դիցուք ունենք $f(c, s) = t$, որտեղ $c \in C, s \in S, t \in T$: Այս դեպքում պետք է տեղի ունենա հետևյալ անհավասարությունները՝

$$\forall c \in C, \forall s \in S, f(c, s) = t, \nexists\, g \;:\; \Pr[\, g(t) = c', c = c' |\, t] > \frac{1}{L}$$

$$\forall c \in C, \forall s \in S, f(c, s) = t, \nexists\, g \;:\; \Pr[\, h(t) = s', s = s' |\, t] > \frac{1}{|S|}$$

2. *Հակադարձելիություն ըստ «գաղտնիքի»*: Դիցուք ունենք $f(c,s)=t$, որտեղ $c\in C, s\in S, t\in T$: Այս դեպքում գոյություն ունի f^{-1} ձևափոխություն այնպես, որ ունենալով t և s արժեքները, կարելի է միարժեքորեն վերականգնել c-ն՝

$$\exists f^{-1}, s.t.\ \Pr[\, f^{-1}(t,s)=c', c=c' | s,t, f(c,s)=t;\,]=1$$

3. *Լրիվություն*: $f: C\times S\to T$ ձևափոխության լրիվության համար պետք է տեղի ունենան հետևյալ պայմանները՝

$$\forall t\in T, \forall c\in C\ , \exists\ s\in S\ :\ f(c,s)=t$$
$$\forall t\in T, \forall s\in S\ , \exists\ c\in C\ :\ f(c,s)=t$$

Մեզ անհրաժեշտ են այնպիսի $O_1: S\to G$ և $O_2: T\to G$ միարժեք հակադարձելի ձևափոխությունները, որոնք «գաղտնիքների» և «անդորրագրային կոդերի» արժեքների տիրույթը արտապատկերում են El-Gamal համակարգի գաղտնագրման G տիրույթ: Նշանակենք ${O_1}^{-1}$: $G\to S$-ով և ${O_2}^{-1}$: $G\to T$ -ով O_1 –ի և O_2-ի հակադարձ ձևափոխությունները, որոնց միջուկ հանդիսանում են համապատասխանաբար O_1 և O_2 արտապատկերումների պատկերները: Ընթացակարգում օգտագործվում է կրիպտոգրաֆիկ անվտանգ հեշ ֆունկցիա, որը նշանակենք *hash*-ով: Ընտրությունների նախնական փուլում կազմվում է n հոգուց բաղկացած կենտրոնական ընտրական հանձնաժողով , որի անդամները բաշխված և (n,m) շեմային եղանակով ստեղծում են ընտրությունների ընդհանուր El-Gamal-ի Y բաց բանալին: Հանձնաժողովի յուրաքանչյուր անդամ տիրապետում է Y բաց բանալուն համապատասխան փակ բանալու x ենթամասին այնպես, որ հանձնաժողովի n անդամներից ցանկացած m հոգին միասին կարող են վերականգնել ամբողջական փակ բանալին: Էլեկտրոնային քվեարկության ամբողջ ընթացակարգը նկարագրվում է հետևյալ կերպ.

<u>Էլ-քվեարկության նոր ընթացակարգ(E-Voting Protocol)</u>

1. Էլեկտրոնային քվեարկության համակարգը(այսուհետ՝ Համակարգ)՝
   (a) Պատահական կերպով գեներացնում է $\boldsymbol{G}$ խմբի $\boldsymbol{r_1, r_2, \dots, r_k}$ էլեմենտներ:
   (b) Հաշվում է այդ էլեմենտների $\boldsymbol{g^{r_1}, g^{r_2}, \dots, g^{r_k}}$ էքսպոնենտները ըստ $\boldsymbol{g}$ հիմքի $\boldsymbol{Z_P^*}$ դաշտում, կոնկատենացնում է ստացված արժեքները և հաշվում է ստացված արժեքի $\mathbf{H1} = \boldsymbol{hash}(\boldsymbol{g^{r_1}||g^{r_2}||\dots||g^{r_k}})$ մատնահետքը:
   (c) Ստացված **H1** մատնահետքը ավելացնում է քվեաթերթիկին և գրում է նաև ընտրողի անդորրագրի վրա:
2. Ընտրողը
   (a) Տեսնելով անդորրագրին ավելացված **H1** կոդը, $\boldsymbol{S}$ բազմությունից պատահական կերպով ընտրում և համակարգ է մուտքագրում k հատ $\boldsymbol{s_1, s_2, \dots, s_k}$ “գաղտնիքներ”՝ $\boldsymbol{s_i}\in_{\boldsymbol{R}}\boldsymbol{S}$:
3. Համակարգը
   (a) Նախօրոք որոշված $\boldsymbol{O_1: S\to G}$ միարժեք ձևափոխության միջոցով ընտրողի բոլոր $\boldsymbol{s_1, s_2, \dots, s_k}$ “գաղտնիքները” արտապատկերում է $\boldsymbol{G}$ ենթախմբի վրա, որից հետո ստացված էլեմենտները գաղտնագրում է El-Gamal համակար-

գով՝ օգտագործելով ընտրությունների $\mathbf{Y}$ բաց բանալին և քվեարկության սկզբում ընտրված $\boldsymbol{r_1, r_2, \dots, r_k}$ պատահական մեծությունները: Համակարգը արդյունքում ստացված $(\boldsymbol{g^{r_1}, O_1(s_1)Y^{r_1}})$, $(\boldsymbol{g^{r_1}, O_1(s_2)Y^{r_1}})$, , $(\boldsymbol{g^{r_k}, O_1(s_k)Y^{r_k}})$ գաղտնագրերը ավելացնում է քվեաթերթիկին:

(b) Հաշվում է այդ գաղտնագրերի մատնահետքը՝
$\boldsymbol{H2 = hash(g^{r_1}||O_1(s_1)Y^{r_1} \,||(g^{r_1}||O_1(s_2)Y^{r_1}||\dots||g^{r_k}||\, O_1(s_k)Y^{r_k})}$
և ավելացնում է այն ընտրողի անդորրագրի վրա:

4. Ընտրողը
   (a) Տեսնելով անդորրագրին ավելացված **H2** կողը, նշում է իր գաղտնի կողերից մեկը: Ընտրված կողի ինդեքսը նշանակենք $\boldsymbol{i}$-ով, որտեղ $\boldsymbol{i} \in [\mathbf{1}, \dots, \boldsymbol{k}]$:
5. Համակարգը
   (a) Ընտրողի անդորրագրի վրա տպում է $\langle \mathbf{j}, \boldsymbol{s_j} \rangle_{\boldsymbol{j=1, j\neq i}}^{\boldsymbol{k}}$ զույգերը: Այսպիսով՝ բացահայտվում են ընտրողի ներմուծած բոլոր "գաղտնիքները" , բացի մեկից, որը նշվել էր ընտրողի կողմից նախորդ քայլի ընթացքում:
   (b) Քվեաթերթիկին է ավելացնում $\langle \mathbf{j}, \boldsymbol{s_j} \rangle_{\boldsymbol{j=1, j\neq i}}^{\boldsymbol{k}}$ զույգերը, ինչպես նաև $\langle \boldsymbol{CP_j} \rangle_{\boldsymbol{j=1, j\neq i}}^{\boldsymbol{k}}$ ոչ-ինտերակտիվ Chaum-Pedersen տիպի ապացույցներ, որոնց շնորհիվ կարելի է համոզվել, որ $\boldsymbol{j}$-րդ գաղտնագիրը իսկապես հանդիսանում է $\boldsymbol{s_j}$-ի գաղտնագրումը :
6. Ընտրողը՝
   (a) Տեսնելով իր ներմուծած գաղտնիքների և համապատասխան ինդեքսների $\langle \mathbf{j}, \boldsymbol{s_j} \rangle_{\boldsymbol{j=1, j\neq i}}^{\boldsymbol{k}}$ զույգերը տպված անդորրագրի վրա, նշում է իր թեկնածուին: Նշված թեկնածուի կողը նշանակենք $\boldsymbol{c}$ -ով, որտեղ $\boldsymbol{c} \in \boldsymbol{C}$:
7. Համակարգը
   (a) Հաշվում է $\boldsymbol{f(c, s_i)}$ ձևափոխության արժեքը: Ստացված $\boldsymbol{t}$ արժեքը ավելացվում է քվեաթերթիկին և ընտրողի անդորրագրին:
8. Ընտրողը
   (a) Հաստատում կամ մերժում է իր քվեարկությունը: Հաստատման դեպքում համակարգը գրանցում է ընտրողի քվեաթերթիկը քվեաթերթիկների տվյալների բազայում և անդորրագիրը տրամադրում է ընտրողին: Մերժման դեպքում ընտրողը նորից քվեարկելու հնարավորություն է ստանում:

Գլխում բերված է այն ստուգումների նկարագրությունը, որոնց շնորհիվ ընտրությունները դառնում են համընդհանուր վերահսկելի: Ապացուցված են հետևյալ պնդումները:

- **Պնդում 1:** Չարագործ համակարգիչն ընտրողի քվեաթերթիկը կարող է փոխել իր նախընտրած թեկնածուի օգտին, սակայն ընտրողի կողմից իր անդորրագրի

օգնությամբ հատուկ ստուգում կիրառելու դեպքում այդ կեղծիքը բացահայտվում է $\mathbf{1}$ հավանականությամբ:

- **Պնդում 2:** Չարագործ համակարգիչն ընտրողի քվեաթերթիկը կարող է փոխել պատահական կերպով՝ առանց իմանալու թե որ թեկնածուի օգտին է այդ քվեաթերթիկը գրանցվելու, սակայն ընտրողի կողմից իր անդորրագրի օգնությամբ հատուկ ստուգում կիրառելու դեպքում այդ կեղծիքը բացահայտվում է $\mathbf{1} - \frac{\mathbf{1}}{\boldsymbol{k}}$ հավանականությամբ:
- **Պնդում 3:** Չարագործը կարող է տվյալների պահոցում ընտրողի քվեաթերթիկը փոխարինել իր նախընտրած թեկնածուի օգտին հանդիսացող քվեաթերթիկով, սակայն ընտրողի կողմից իր անդորրագրի օգնությամբ հատուկ ստուգում կիրառելու դեպքում այդ կեղծիքը բացահայտվում է $\mathbf{1}$ հավանականությամբ:

Քվեների գաղտնիությունը ապահովելու նպատակով քվեաթերթիկները անանունացվում(անոնիմացվում) են MIX ցանցերի օգնությամբ: Դրա համար քվեաթերթիկներից հեռացվում են բոլոր դաշտերը՝ բացի անդորրագրային $\boldsymbol{t}$ կոդից և $\boldsymbol{s_i}$ գաղտնիքին համապատասխանող գաղտնագրից: Ստացված յուրաքանչյուր $\{t, \mathcal{E}\}$ քվեաթերթիկ այնուհետև ձևափոխվում է հետևյալ կերպ.

1. t արժեքը $O_2: T \to G$ ձևափոխության միջոցով արտապատկերվում է G խմբի էլեմենտի: Ստացված $O_2(t)$ էլեմենտը բարձրացվում է քառակուսի աստիճան և գաղտնագրվում է Y բանալիով El-Gamal ալգորիթմի օգնությամբ՝ օգտագործելով $r = 1$ արժեքը: Ստացված գաղտնագիրը նշանակենք
$$\mathcal{E}_1 = (g^1, [O_2(t)]^2 Y^1) \stackrel{\text{def}}{=} (E_1, F_1)$$
2. Հաշվվում է $O_2(t)$-ի հակադարձը G խմբում: Ստացված $[O_2(t)]^{-1}$ –ի և $\mathcal{E} = (g^r, O_1(s)Y^r)$ գաղտնագրի օգնությամբ հաշվվում է
$$\mathcal{E}_2 = (g^r, O_1(s)[O_2(t)]^{-1}\ Y^r) \stackrel{\text{def}}{=} (E_2, F_2)$$
գաղտնագիրը:
3. $[O_2(t)]$ –ի և $\mathcal{E} = (g^r, O_1(s)Y^r)$ գաղտնագրի օգնությամբ հաշվվում է $\mathcal{E}_3 = (g^r g^1, O_1(s)O_2(t)\ \ Y^r Y^1) = (g^{r+1}, O_1(s)O_2(t)\ \ Y^{r+1})$ գաղտնագիրը:

Նկատենք որ ստացված երեք գաղտնագրերի միջև տեղի ունի հետևյալ կապը՝
$$\mathcal{E}_3 = \mathcal{E}_1 \circ \mathcal{E}_2 = (E_1 \cdot E_2, F_1 \cdot F_2)$$

MIX գործընթացի ժամանակ յուրաքանչյուր MIX հանգույց իրականացնում է հետևյալ MIX ալգորիթմը.

<u>MIX ալգորիթմ</u>

- Որպես մուտքային տվյալներ վերցվում է $\{(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3)_i\}_{i=1}^N$ քվեաթերթիկների բազմությունը:

- Ընտրվում է պատահական էլեմենտների $\{r_1^i\}_{i=1}^N$ բազմությունը:
- Ընտրվում է պատահական էլեմենտների $\{r_2^i\}_{i=1}^N$ բազմությունը:

Յուրաքանչյուր $(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3)_i$, $i \in [1, N]$ քվեաթերթիկի համար `

- Վերագաղտնագրվում է առաջին $\mathcal{E}_1$ գաղտնագիրը՝ օգտագործելով r_1^i պատահական արժեքը: Մենք բաց կթողնենք r_1^i –ի i ինդեքսը՝ բանաձևերի տեսքը չբարդացնելու համար: Արդյունքում ստացվում է
$$\mathcal{E}'_1 = \boldsymbol{\mathcal{RE}}_Y(\mathcal{E}_1 : r_1) = (g^{r_1+1}, [O_2(t)]^2 Y^{r_1+1}) \stackrel{\text{def}}{=} (E'_1, F'_1)$$
- Վերագաղտնագրվում է երկրորդ $\mathcal{E}_2$ գաղտնագիրը՝ օգտագործելով r_2^i պատահական արժեքը: Մենք բաց կթողնենք i ինդեքսը: Արդյունքում ստացվում է
$$\mathcal{E}'_2 = \boldsymbol{\mathcal{RE}}_Y(\mathcal{E}_2 : r_2) = (g^{r_2+r}, O_1(s) \cdot [O_2(t)]^{-1} Y^{r_2+r}) \stackrel{\text{def}}{=} (E'_2, F'_2)$$
- Վերագաղտնագրվում է երրորդ $\mathcal{E}_3$ գաղտնագիրը՝ օգտագործելով $r_1^i + r_2^i$ պատահական արժեքը: Մենք բաց կթողնենք i ինդեքսը: Արդյունքում կստացվի՝
$$\mathcal{E}'_3 = \boldsymbol{\mathcal{RE}}_Y(\mathcal{E}_3 : r_1 + r_2) = (g^{r_1+r_2+r+1}, O_1(s) \cdot [O_2(t)]\, Y^{r_1+r_2+r+1}) \stackrel{\text{def}}{=} (E'_3, F'_3)$$
- Ընտրվում է կամայական $\pi : [1,2, \dots N] \to [1,2, \dots, N]$ տեղափոխություն: Քվեաթերթիկների $\{(\mathcal{E}'_1, \mathcal{E}'_2, \mathcal{E}'_3)_i\}_{i=1}^N$ բազմության վրա կիրառվում է ընտրված տեղափոխությունը և ելքում վերադարձվում է ստացված բազմությունը:

Ինչպես երևում է, եթե MIX հանգույցը քվեաթերթիկների դիմակավորումը կատարի ըստ վերևում նշված ալգորիթմի, ապա նորից տեղի կունենա հետևյալ հավասարությունը.
$$\mathcal{E}'_3 = \mathcal{E}'_1 \circ \mathcal{E}'_2 \stackrel{\text{def}}{=} (E'_1 \cdot E'_2, F'_1 \cdot F'_2)$$

Յուրաքանչյուր MIX հանգույց բացի MIX ալգորիթմը իրականացնելուց, պարտավոր է նաև տալ իր կատարած MIX գործողության ճշգրտության ստուգման ապացույց: Յուրաքանչյուր հանգույցի համար նշանակենք $A = \{(\mathcal{E}_1)_i\}_{i=1}^N$, $B = \{(\mathcal{E}_2)_i\}_{i=1}^N$, $C = \{(\mathcal{E}_3)_i\}_{i=1}^N$ և $A' = \{(\mathcal{E}'_1)_i\}_{i=1}^N$, $B' = \{(\mathcal{E}'_2)_i\}_{i=1}^N$, $C' = \{(\mathcal{E}'_3)_i\}_{i=1}^N$:

MIX գործընթացի ճշգրտության ապացուցման ալգորիթմ

1. MIX հանգույցը, հանդիսանալով ԱՊԱՑՈՒՅՑՈՂ, El-Gamal-ի հիման վրա կառուցված միաչափ MIX ցանցերի ստուգման Neff-ի հայտնի ալգորիթմի օգնությամբ ապացուցում է ՍՏՈՒԳՈՂԻՆ, որ A' բազմությունը ստացվել է A բազմության վերագաղտնագրված էլեմենտների տեղափոխությունից: Նշանակենք այս հարաբերությունը որպես $A \approx A'$: Նույն կերպ ապացուցում է նաև, որ $B \approx B'$ և $C \approx C'$:
2. ՍՏՈՒԳՈՂ-ը, վերցնելով $A = \{(\mathcal{E}_1)_i\}_{i=1}^N$, $B = \{(\mathcal{E}_2)_i\}_{i=1}^N$, $C = \{(\mathcal{E}_3)_i\}_{i=1}^N$ և $A' = \{(\mathcal{E}'_1)_i\}_{i=1}^N$, $B' = \{(\mathcal{E}'_2)_i\}_{i=1}^N$ և $C' = \{(\mathcal{E}'_3)_i\}_{i=1}^N$ բազմությունները, ստուգում է, արդյոք տեղի ունի հետևյալ հավասարությունները՝

- $A \approx A'$; $B \approx B'$; $C \approx C'$
- $(\mathcal{E}'_1)_i \circ (\mathcal{E}'_2)_i = (\mathcal{E}'_3)_i \quad \forall\, i \in [1, \dots, N]$

Գլխում բերված են MIX գործընթացում հնարավոր կեղծիքների նկարագրությունները և MIX հանգույցի տրամադրած ապացույցի միջոցով նման կեղծիքների հայտնաբերումը: Ապացուցված է հետևյալ պնդումը.

- **Պնդում 4:** MIX ցանցի մաս հանդիսացող չարագործ հանգույցը ընտրությունների արդյունքները խեղաթյուրելու նպատակով կարող է փոխարինել գրանցված քվեաթերթիկները: Ցանկացած մարդ կարող է բացահայտել նման կեղծիքները $\mathbf{1}$ հավանականությամբ՝ կատարելով հատուկ ստուգումներ:

MIX ցանցի գործունեության ավարտից հետո ընտրական հանձնաժողովի անդամներից յուրաքանչյուրը իր գաղտնի բանալով կատարում է քվեաթերթիկների երեք գաղտնագրերի մասնակի ապագաղտնագրում: Վերջին մասնակի ապագաղտնագրումից հետո բոլոր գաղտնագրերը ամբողջովին ապագաղտնագրվում են և բացահայտվում են հետևյալ երեք $[\boldsymbol{O_2(t)}]^{\mathbf{2}}$, $\boldsymbol{O_1(s)} \cdot [\boldsymbol{O_2(t)}]^{-\mathbf{1}}$, $\boldsymbol{O_1(s)} \cdot [\boldsymbol{O_2(t)}]$ էլեմենտները: Առաջին էլեմենտից ստացվում է $\boldsymbol{O_2(t)}$-ն, այնուհետև $\boldsymbol{O_2(t)}$-ի օգնությամբ երրորդ էլեմենտից ստացվում է $\boldsymbol{O_1(s)}$-ը: Դրանից հետո $\boldsymbol{{O_1}^{-1}}$ և $\boldsymbol{{O_2}^{-1}}$ հակադարձ ձևափոխությունների օգնությամբ վերականգնվում են $\boldsymbol{t}$ և $\boldsymbol{s}$ արժեքները: Ստացված արժեքներից $\boldsymbol{f^{-1}}$ հակադարձ ձևափոխության միջոցով վերականգվում է համապատասխան թեկնածուի $\boldsymbol{c = f^{-1}(t, s)}$ կողը և տվյալ թեկնածուի ստացած ձայների քանակը ավելանում է մեկով: Ապացուցված է հետևյալ պնդումը՝

- **Պնդում 5:** Ընտրական հանձնաժողովի յուրաքանչյուր անդամ ապագաղտնագրման գործողության հետ մեկտեղ տալիս է ապագաղտնագրման գործողության ճշգրտության ապացույց: Ցանկացած ոք կարող է ստուգել այդ ապացույցի ճշգրտությունը, ինչի շնորհիվ ապագաղտնագրման ժամանակ տեղի ունեցած ցանկացած անճշտություն բացահայտվում է $\mathbf{1}$ հավանականությամբ:

Ապացուցված բոլոր 5 պնդումները միասին ցույց են տալիս, որ առաջարկված էլեկտրոնային քվեարկության համակարգը ապահովում է համընդհանուր վերահսկելիություն՝ միաժամանակ չխախտելով քվեների գաղտնիությունը: Գլխում նկարագրված են բերված ընթացակարգին համաձայն քվեարկությունների երկու տարբեր կիրառական մոտեցումներ: Այդ մոտեցումներից մեկի հիման վրա իրականացվել է էլեկտրոնային քվեարկությունների կազմակերպման SecureVoting համակարգը, որի նկարագրությունը տրված է Չորրորդ գլխում:

Երրորդ գլխում Այս գլխում նկարագրված է Հայաստանում առաջին անգամ 2012թ-ի մայիսի խորհրդարանական ընտրությունների ժամանակ գործարկված էլեկտրոնային քվեարկության համակարգը, որի օգնությամբ Հայաստանի՝ արտերկրում դիվանա-

գիտական ծառայության մեջ գտնվող քաղաքացիները կարող էին մասնակցել ընտրություններին: Ուսումնասիրվել է այդ համակարգի հիմքում ընկած ընթացակարգի անվտանգության հատկանիշները և ցույց է տրվել այդ համակարգի խոցելիությունը երեք հիմնական հարձակումների նկատմամբ՝

- Հարձակում 1: Ընտրություններից հետո գաղտնագրեր գեներացնող կազմակերպությունը արդեն իսկ գրանցված ցանկացած քվեաթերթիկ կարող է ցանկացած պահի ապագաղտնագրել և բացահայտել համապատասխան քվեն:
- Հարձակում 2: Ապագաղտնագրումից հետո համակարգի տվյալների պահոցին հասանելիություն ունեցող ցանկացած ոք կարող է բացահայտել քվեի և ընտրողի կապը, այսինքն քվեի գաղտնիությունը բացահայտվում է:
- Հարձակում 3: Ընտրությունների ավարտից հետո մինչև քվեաթերթիկների ամփոփումը ընկած ժամանակահատվածում քվեաթերթիկների պահոցին հասանելիություն ունեցող ցանկացած չարագործ կարող է կամայական կերպով փոխել քվեաթերթիկները և մնալ չբացահայտված: Ընտրությունների ամբողջականությունը չի պահպանվում:

Այդ էլեկտրոնային քվեարկությանը մասնակից ընտրողների թիվը չի կարող գերազանցել մի քանի հարյուրը, և մինչև ընտրությունների ավարտը թույլատրվում է բազմակի քվեարկություն: Հաշվի առնելով այս հանգամանքները՝ առաջարկվել է քվեարկության պարզ և մատչելի ինտերֆեյս ապահովող համակարգի կառուցման ընթացակարգ, որը ապահովում է քվեների գաղտնիությունը և ընտրությունների ամբողջականությունը՝ ընտրողին տալով իր քվեաթերթիկի ճիշտ գրանցման և հաշվարկի վերահսկելիության մեխանիզմներ: Համակարգը հիմնված է Paillier-ի բաց բանալով գաղտնագրության համակարգի և Baudron-ի կրիպտոգրաֆիկ հաշվիչների հիման վրա: Ընտրություններից առաջ վստահված անձինք բաշխված շեմային եղանակով գեներացնում են ընտրությունների Paillier գաղտնագրության համակարգի բաց բանալին, որը իրենից ներկայացնում է (N, g) զույգ, որտեղ $g^N \equiv 1\, mod\, N^2$ և $N = P \cdot Q$, իսկ P-ն և Q-ն մեծ պարզ թվեր են (512 բիթ կամ ավել): Դիցուք թեկնածուների քանակը հավասար է z: Յուրաքանչյուր $j \in [1, z]$ թեկնածուի համապատասխանեցվում է $c_j = 2^{(j-1)M}$ կոդը, որտեղ $M = \frac{|N|}{z}$: Ընտրողների նույնականացման համար օգտագործվում է գաղտնաբառ-գաղտնանուն զույգ, որը իրավասու ընտրողը ձեռք է բերում ԿԸՀ-ից մինչև ընտրությունները: Նույնականացման փուլից հետո ընտրողը քվեարկում է համաձայն ներքևում նկարագրված ընթացակարգի:

<u>Էլեկտրոնային քվեարկության ընթացակարգ</u>

1. Ընտրողը քվեարկում է՝ նշելով իր նախընտրած $j \in [1, z]$ թեկնածուին:
2. Համակարգը՝
   - ընտրությունների բաց բանալով գաղտնագրում է նշված j-րդ թեկնածուի համապատասխան $c_j = 2^{(j-1)M}$ կոդը՝ օգտագործելով

պատահական կերպով ընտրված $r \in Z_N$: Ստացված $\boldsymbol{\mathcal{E}} = g^{c_j} r^{\mathrm{N}} \mathrm{mod\ N}^{\,2}$ գաղտնագիրը ավելացնում է քվեաթերթիկին:

- գեներացնում է 0-ինֆորմատիվ $\boldsymbol{P}$ ապացույց, ինչի շնորհիվ ցույց է տրվում, որ $\boldsymbol{\mathcal{E}}$ գաղտնագրի թաքցրած տեքստը իսկապես պատկանում է $C = \{\, 2^{(j-1)M} \}_{j=1}^{z}$ բազմությանը:
- հաշվում է $\mathrm{H1} = hash(\boldsymbol{\mathcal{E}})$ և $\mathrm{H2} = hash(\boldsymbol{P})$ մատնահետքերը և ավելացնում է ընտրողի անդորրագրի վրա:
- Ստորագրում է ընտրողի քվեաթերթիկը և անդորրագիրը:

3. Ընտրողը հաստատում կամ մերժում է քվեարկությունը: Հաստատման դեպքում ստորագրված քվեաթերթիկը գրանցվում է քվեաթերթիկների տվյալների պահոցում, իսկ անդորրագիրը նախօրոք հաստատված կապուղու միջոցով, որը կարող է լինել e-mail կամ տպիչ, տրամադրվում է ընտրողին: Մերժման դեպքում ընտրողը հնարավորություն է ստանում նորից քվեարկելու:

Այսքանով ավարտվում է քվեարկության փուլը: Գրանցված քվեաթերթիկները ինտերնետի օգնությամբ դիտելու համար հասանելի են բոլորին: Գլխում բերված են քվեաթերթիկների ամբողջականության ստուգման մեխանիզմները:

Քվեաթերթիկների ապագաղտնագրման և քվեների հաշվարկի համար քվեաթերթիկներից վերցվում են գաղտնագրերը և բաց կերպով հաշվարկվում է դրանց արտադրյալը: Paillier-ի գաղտնագրության համակարգը օժտված է ադիտիվ հոմոմորֆիկության հատկությամբ, ինչը արտահայտվում է հետևյալ բանաձևով՝

$$\boldsymbol{\mathcal{E}}_{pk}(m_1 ; r_1) \times \boldsymbol{\mathcal{E}}_{pk}(m_2 ; r_2) = g^{m_1} \cdot {r_1}^N \ mod\ N^2 \times\ g^{m_2} \cdot {r_2}^N \ mod\ N^2 \ = g^{m_1+m_2} \cdot {r_1}^N \cdot {r_2}^N \ mod\ N^2 = \boldsymbol{\mathcal{E}}_{pk}(m_1 + \ m_2; r_1 \ \cdot r_2)$$

Բոլոր գաղտնագրերի արտադրյալը հաշվելուց հետո ստացված գաղտնագրի համար տեղի կունենա հետևյալ հավասարությունը.

$$\boldsymbol{\mathcal{E}} = \prod \boldsymbol{\mathcal{E}}_{\,i} = Enc\left(\sum c_i\right) = Enc(\sum_{j=1}^{z} l_j 2^{(j-1)M})$$

Այստեղ $\sum_{j=1}^{z} l_j$ գումարը հավասար է հաշվարկին մասնակցած քվեաթերթիկների թվին, որտեղ l_j-ն հանդիսանում է j-րդ թեկնածուի օգտին գրանցված ձայների քանակը:

Ստացված $\boldsymbol{\mathcal{E}}$ գաղտնագիրը այնուհետև ապագաղտնագրվում է ընտրական հանձնաժողովի քվորում կազմող անդամների կողմից: Ապագաղտնագրման ճշգրտությունը կարող է ստուգել ցանկացած մարդ: Բացահայտված $\sum_{j=1}^{z} l_j 2^{(j-1)M} = T$ թվից կարելի է ստանալ բոլոր թեկնածուների օգտին գրանցված քվեների քանակը: T թվի առաջին M բիթով ստացվող թիվը արտահայտում է առաջին թեկնածուի օգտին գրանցված քվեների քանակը, հաջորդ M բիթով ստացվող թիվը՝ երկրորդ թեկնածուի քվեների քանակը, և այսպես շարունակ:

Չորրորդ գլխում ներկայացված է էլեկտրոնային քվեարկություններ իրականացնելու համար ստեղծված SecureVoting համակարգի ընդհանուր նկարագրությունը: Համակարգը հնարավորություն է ընձեռում իրականացնել ընտրությունների

նշանակում, քվեարկություն, քվեների անանունացում և ձայների հաշվարկ: Ընտրությունների նշանակման փուլի իրականացման գլխավոր քայլեր են.

- Ընտրությունների կազմակերպչի գրանցում SecureVoting համակարգում, ինչը կարող է իրականացվել նաև Facebook սոցիալական ցանցի միջոցով:
- Կազմակերպչի կողմից ընտրությունների պարամետրերի(ընտրական հարցերի ցուցակ, յուրաքանչյուր հարցի համար պատասխանների/թեկնածուների նշում) մուտքագրում SecureVoting համակարգ:
- Կազմակերպչի կողմից Ընտրություններին մասնակցելու իրավասու ընտրողների ցուցակի կազմում:
- Կազմակերպչի կողմից Վստահված անձանց նշանակում և համապատասխան բաց բանալիների ձեռքբերում:
- Կազմակերպչի կողմից Ընտրությունների բաց գաղտնագրության բանալիի կառուցում վստահված անձանց բանալիներից:

Քվեարկության փուլի ժամանակ յուրաքանչյուր ընտրողի համար կատարվում են հետևյալ երկու քայլերը.

- Ընտրողի նույնականացում:
- Ընտրողի քվեարկություն՝ համաձայն Էլ-քվեարկության նոր ընթացակարգի, որտեղ օգտագործվում է թեկնածուների ցուցակի վրա ընտրողի կողմից պատահական տեղափոխություններ կիրառելու մեթոդը:

Երրորդ փուլի՝ քվեների անոնիմացումը տեղի է ունենում MIX ցանցի օգնությամբ, երբ առաջին փուլում գրանցված բոլոր վստահված անձինք հերթով իրականացնում են քվեաթերթիկների վերագաղտնագրում և տեղափոխություն: Չորրորդ փուլը իրականացվում է քվեների անոնիմացման փուլից հետո: Բոլոր վստահված անձինք համատեղ վերականգնում են ընտրությունների բաց բանալուն համապատասխան գաղտնի բանալին, որի միջոցով տեղի է ունենում քվեների ապագաղտնագրում և ձայների հաշվարկ: Գլխում մանրամասն դիտարկված են բոլոր քայլերը: Ներկայացված են ինտերֆեյսային որոշ լուծումներ:

Հիմնական արդյունքներն ու եզրակացությունները

Աշխատանքի հիմնական արդյունքներն են.

- Առաջարկվել է էլեկտրոնային քվեարկության նոր ընդհանրացված ընթացակարգ, որը տարբերվում է մինչ այժմ գոյություն ունեցող ընթացակարգերից այն հանգամանքով, որ քվեարկության համակարգը բոլոր անհրաժեշտ գաղտնագրումները կատարում է մինչև ընտրողի կողմից իր նախընտրած թեկնածուի նշումը[1]:
- Վերլուծվել է առաջարկված ընթացակարգի անվտանգության հատկանիշները, ցույց է տրվել, որ առաջարկված ընթացակարգը ապահովում է ընտրությունների համընդհանուր վերահսկելիություն և քվեների գաղտնիություն[2][4]:

- Առաջարկված ընթացակարգի համար կառուցվել է քվեաթերթիկների անոնիմացման նոր MIX ցանց, որը ապահովում է քվեաթերթիկների բացարձակ գաղտնիություն և MIX գործընթացի վերահսկելիություն[3]:
- Տրվել է էլեկտրոնային քվեարկություններ իրականացնելու երկու կիրառական լուծում՝ համաձայն առաջարկված ընդհանրացված ընթացակարգի[1][4]:

Ատենախոսության թեմայի շրջանակներում հրապարակված աշխատություններ

1. G. Khachatryan, A. Jivanyan, "Secure and safe E-Voting system based on public key cryptography", In Proceedings of WAITC'2010, Armenian-Russian-German Workshop on Applications of Information Theory, Coding and Security, Yerevan, Armenia pp.25-30, 2010.
2. G. Khachatryan, A. Jivanyan, "New E-Voting Protocol Based on Voter's Secrets", In Proceedings of CSIT2011 Eighth International Conference on Computer Science and Information Technologies. Yerevan, Armenia, pp.15-19, 2011.
3. G. Khachatryan, A. Jivanyan, "Hybrid Self-Proving Mix Network", In Proceedings of CSIT2011 Eighth International Conference on Computer Science and Information Technologies. Yerevan, Armenia, pp.142-145, 2011.
4. A. Jivanyan, "A New Approach to Receipt-Free E-Voting" In Journal of Mathematical Problems of Computer Science 37, 2012. Yerevan, Armenia, pp.75-82, 2012.

Дживанян Арам Арутюнович

Разработка и реализация новых систем электронных голосований

РЕЗЮМЕ

Более 20 лет проводятся научно-исследовательские работы по созданию криптографических систем электронного голосования, с помощью которых станет возможным проводить свободные выборы без возможных фальсификаций. Доверие к выборам, осуществляемым посредством таких систем, должно основываться не на безопасности этих систем, а на математических свойств протокола выборов, которая лежит в основе этих систем. Протокол должен иметь такие математические свойства, которые дадут возможность при помощи специальных проверок выявлять нарушения на любом этапе процесса выборов. В то же время протокол не должен в какой-то момент даты возможность раскрывать тайный голос избирателя. Первую такую процедуру, позволяющую реализовать контролируемые выборы, вне зависимости от безопасности используемых устройств, была предложена известным криптографером Chaum-ом. После этого было создано множество криптографических систем голосования. В таких системах, чтобы сохранить секретность голосов, в основном использовалось два типа криптографических подходов. Первое – это придавание анонимности бюллетеням с помощью MIX–сетей. Второе–агрегатный подсчет голосов при помощи гомоморфных криптографических систем.

Криптографические системы реально в выборах начали использоваться недавно, и таких примеров немного. Особенно характерно использование системы Scantegrity на выборах в городе Takoma Park в 2009 году, где были использованы специальные бумажные бюллетени, а придача анонимности голосам и подсчет производился с помощью криптографических методов. Одной из самых развитых систем на сегодняшний день является система Pret-A-Voter, которая будет использована на выборах в штате Виктория, в Австралии. Обе системы используют бумажные бюллетени, полученные при помощи специальных криптографических методов, которые позволяют избирателю после выборов проверить, не подвергался ли его голос фальсификации. Однако факт использования бумажных бюллетеней уже дает возможность проведения различных нападений, с помощью которых удасться изменить результаты выборов. Еще одной из самых развитых систем электронных выборов является использованная в 2011 году в Норвегии система, которая не использует бумажных бюллетеней, но в то же время обеспечивает общий контроль над выборами. Этот контроль становится возможным с помощью специальных квитанций, которые выдаются избирателю после выборов, однако в то же время с помощью этой квитанции появляется возможность раскрыть голос избирателя, то есть эта система не обеспечивает полной секретности. Существуют также много других систем, которые представляют собой большой теоретический интерес, однако не нашли своего применения ввиду своей неэффективности или непрактичности.

Приведенный выше анализ показывает актуальность задачи разработки нового криптографического протокола электронних голосований, который обеспечивает полную секретность голоса и дает общий контроль над избирательним процессом.

Целью данной работы является разработка нового протокола электронних голосований, который

- Не полагается на бумажные бюллетени.
- Обеспечивает общий контроль над избирательним процессом.
- Гарантирует полную секретность голоса.
- Обеспечивает вычислительно эффективные процедуры для анонимизации голосов и подсчета.
- Предоставляет удобный интерфейс для ползователя.
- Не требует специальных электронных машин или сканеров, которые повышают стоимость выборов.

Следующей целью данной работы является анализ аспектов безопасности электронной системи голосования, которая используется армянскими дипломатамы и членамы их семей во время армянских национальных голосований.

Основные результаты диссертационной работы следующие:

- Был разработан новый обобщенный протокол выборных процедур, которая отличается от существующих протоколов тем, что ненадежная машина выборов делает все необходимые операции зашифрования до реального выбора избирателя[1].
- Были исследованы свойства безопасности предлагаемого протокола и было показано, что предлагаемый протокол обеспечивает полную секретность голосов и дает общий контроль над избирательним процессом[2][4].
- Был построен новый анонимизирующий сеть специально для предлагаемого протокола, который гарантирует полной конфиденциальности голосов во время анонимизации голосов и дает возможности эффективным методом генерировать доказательства точного выполнения этой процедуры[3].
- Были разработаны два различных прототипов обобщенного протокола, которые обеспечивают дружественные интерфейсы голосования для ползователей[1][4].

Aram Jivanyan

Design and development of new e-voting systems

RESUME

For more than twenty years of scientific research work has been carried out for developing cryptographic e-voting systems, which will enable to hold fair elections without cheating. The trust on such systems must be based not on the machines which are running the system, but on the mathematical properties of the underlying voting protocol. It is considered that all voting machines, which are used during elections, are non-trusted, and the voting protocol must mathematically ensure that any cheating appeared at any step of election process will be discovered after appropriate checks. The first protocol, which had shown theoretically the possibility of holding verifiable and secure elections, was proposed by D. Chaum at 1980. Since than hundreds of different voting protocols were invented by researchers, which all are trying to guaranty the necessary security and secrecy properties of voting. The vote secrecy in cryptographic voting system can be ensured by two different cryptographic methods: The first method is to anonyme all ballots with help of secure Mix Networks. The second approach is to compute all votes in aggregated manner with help of homomorphic encryption schemes. The cryptographic voting systems have started to be used in real-life large scale elections only recently and there are only a few examples of success stories. Among them it is worth mentioning the elections of Takoma Park City in USA, where the cryptographic voting system called ScantegrityII had been used. ScantegrityII uses special paper ballots, on which the voter marks his/her choice with special pen. A special invisible code printed on the ballot is revealed on the ballot after marking it with special pen. The voter can rewrite the code on special part of ballot and take the part with himself out of polling station as a receipt. The receipt allows the voter to verify the consistency of his/her vote after voting. The next system in the list of modern most advanced voting systems is the Pret-A-Voter system developed by Peter Ryan. It is going to be used in the Victoria State Elections in Australia at 2014. Pret-A-Voter is also based on special paper ballots, but the anonymization and the tabulation of votes is done with help of mix networks. However all voting systems, which are using paper ballots, are vulnerable to some kind of attacks, which can break the election integrity. One of the most critical attacks against paper ballot based voting system is the chain-voting attack, and both Scan-te-grity and Pret-A-Voter are vulnerable against that attack. The next advanced e-voting system worth mentioning was used in Norway 2011 governmental elections. The system does not require paper ballots and the same time provides universal verifiability of elections. After casting the vote special secret receipts are given to voter which helps the voter to verify that his vote was casted by intrusted voting computer as intended by voter and was recorded in the database as was casted. The Norwegian voting system also uses mix networks for ballot anonymization. However this system does not provide receipt-freeness, which means that the voter's receipts can violate the secrecy of his vote. This is serious breakdown of the system's security. There exists also number of voting systems not mentioned above which all have great theoretical importance but are far from being practical in order to be used during large-scale elections. The above discussion demonstrates the urgency of the task of developing new cryptographic e-voting protocol, which provides fully secrecy of the votes and universal verifiability of election process.The purpose of this work is to design a new e-voting protocol, which

- Does not rely on paper-based ballots.
- Provides universal verifiability of election process.
- Guaranties fully secrecy of votes.

- Provides computationally efficient procedures for votes counting and anonymization.
- Ensures usability for voters by providing user-friendly voting interface.
- Does not require special e-voting machines or scanners in order not to raise the cost of elections.

The next purpose of this work is to analyse the security aspects of the e-voting system recently launched in Armenia which is used by Armenian diplomats and their family members during Armenian national elections.

The main results of the work are the followings

- A generalized e-voting protocol was proposed, which differs from the existing methods by the fact that all necessary encryption operations are done by the untrusted voting machine before the voter mentions his/her actual choice[1].
- The security properties of the proposed protocol were investigated and it was shown that the proposed protocol provides secrecy of votes and universal verifiability of election process[2][4].
- A new Mix Network was constructed specially for the proposed protocol, which guaranties fully privacy of votes during mix process and provides effective proof of shuffle [3].
- Two different interpretations of the generalised protocol were investigated which provide practical user-friendly voting interfaces[1][4].

Ծավալը՝ 20 էջ: Տպաքանակը՝ 100:
ՀՀ ԳԱԱ ԻԱՊԻ կոմպյուտերային պոլիգրաֆիայի լաբորատորիա:
Երևան, Պ. Սևակի 1