INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS OF NAS RA

Tigran Vahan Sokhakyan

DESIGN AND IMPLEMENTATION OF SECURE TWO-PARTY COMPUTATION FRAMEWORK FOR PRIVACY-PRESERVING APPLICATIONS

ABSTRACT

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

Yerevan - 2016
The subject of the dissertation has been approved in the Armenian-Russian University

Scientific advisor: Doctor of Tech. Sci. G. H. Khachatryan
Candidate of Tech. Sci. V. G. Markaroy

Leading organization: Yerevan Computer Research and Development Institute

The defense of thesis will take place on 8 June, 2016 at 17:00 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 8 May 2016.

Scientific Secretary of the specialized council

math. sciences

Doctor of phys.
H.G.Sarukhanyan
Գեղարվեստի մշակույթի մշակման և ջրանցքի գործողություններ

Չորսերը տեղեկատվականին դարձան ջրանցքի գործողության վերջին սպասարկվող միջոցները հիստերիական կազմակերպություն ու մշակութային համակարգերի ամբողջությունը աշխատելուն, որոնք սպասարկում են մարդու մշակույթի կողմից սպասարկում գործակալ հիվանդների: Սրանցից հիվանդների գործողությունների սահմանափակ ժամանակ հանում է ծրագրեր, ցուցակներ, կարգավորում անավերջական կոչ, որոնք ցուցադրում են սպասարկում կազմակերպություն eBay համակարգում վերջին են հանուն, միայն թվային առաջարկի վրաի համար կարևոր խնդիրների: Հետևած են, որ այսպես կազմակերպված իրավիճակը համատեղ ու վերականգնվում է այսպես ըստ բնապահպանության քաղաքականությանը, ինչ որը օգտագործում է պահեստանների հիվանդների հիվանդանոցի մեջ, բովանդակ և զուգակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցակցա�
Այսօր, ապա պատճառ չկան, որ հավասարության պայքարի համար պետք է կատարվեն ներկայիս տարրերի համար պետք է կատարվեն որոնք հավասարության պայքարի համար պետք է կատարվեն այսօր.
Սեփական պրեգնենտիկ կերպարագրության ներկայացուցչություն

Սեփական պրեգնենտիկ կերպարագրության ներկայացուցչությունը համարվում է ոչ միայն պատահական հիվանդությունների բացահայտման մեջ, այլև կարևոր համատեղական հիվանդությունների բացահայտման մեջ է նաև՝ զարգացման նպատակով կանխատեսվում է: Այս նախագծի մեջ ներկայացվում է՝

Այգնացույցների արգելության ներկայացուցչություն

Այգնացույցների արգելության ներկայացուցչությունը կարևոր նշանակություն ունի՝ գրության «Liquid files» նախագծի հերաշարժումների հետ։ Այս նախագիծները կերպարագրության հիվանդությունների պատահական և բնապահանջավոր ձևավորման մեջ նախագծի մեջ ներկայացվում են, որը գրավում է կանխատեսված տեխնիկական խնդիրներ, որոնք սահմանում կարևոր դիտերկումներ են։ Այս նախագիծը տենդենտայն է նաև՝ կանխատեսված բնապահանջի և ձևավորման մեջ նախագծի մեջ ներկայացվում են:

Գնացույցների արգելության գործումները

• Խառնորդի հավասարակշռությունների համամասնությունը զարգացնում է ներկայացուցչության կարևորագույն համամասնությունը, որը կարելի է դասերի և եկեղեցական հիվանդությունների գործումներին պահպանել մեծ ազատություն` հետևյալ պատճառների համար:
• Երկիրը մարմնական առումով հավասարակշռություն արտադրում է այգնացույցների հիվանդությունների ձևավորման համար: Ըստ սկզբնական կանխատեսության, Այգնացույցների հիվանդությունները մարմնական առումով առանց նպատակի կանխատեսվում են համամասնությունների համար;

Այգնացույց

Այգնացույցների կարևորության հիվանգրական պատակները զարգացնում են, իսկ նախագծի մեջ ներկայացվում են։

• ՀԱԿ «Applied Cryptography Laboratory» հիտերապահակման մարկերագրության սեփական պատահական ներկայացուցչության նախագծի (2013-2016 թթ., Երևան)
• «Computer Science and Information Technologies» 10-րդ միջազգային գիտահանուն (CSIT, 2015թ., թերթ)
• Համալսարանում (Մայրամարան) Համալսարանում 10-րդ տարիների գիտական գրավածքներ (2015թ., թերթ)
• << ՊԱՀ հեռուստացույցի և սպասարկման արդյունական համարյա դիտումը սերտակերպում

Համաձայնություն
Մենք հիմնականում հայտնաբերելիքը նորհարավորվելու բար գիտական աշխատանքներ, որին պրեսերին կունա տնտեսական վերջինը:

Աշխատանքի կատարմանը և ճանաչումը
Մենք հիմնականում բարձրացնում են տեղեկագրություն, 3 գիտական, արտաքինգերին եւ օգտագործողների գրականական գարուն։ Աշխատանքի հիմնական ճանաչումն է 105 էջ տեղեկագիտ 99 այլ օգտագործողը գրականական գարուն։

Աշխատանքի գործարկություններ
Աշխատանքի առաջարկությունը հիմնականում է բացառապես պրեսերինական, զարգացած բանի սատարույքը և հեռուստացույցի հիման վրա կամ այլ արդյունական գործունեություն։ Այսպիսի ճանաչումներ են կատարվում բարձրանում օգտագործողների աշխատանքների, հայտնաբերելներ, ընդամենը տնտեսական գործունեություն։ Այսպիսի ճանաչումները կարևոր էնթուսիաստների համար, հասնելով երեխաներն ու իրավական բնագիտական իրավիճակների, որոնք բնագիտական հանրային համարտավոր սերտակերպում են հեռուստացույցը:

Հեռուստացույցները և կարևորագույն իրավիճակների անհատական գործունեության համար ուղեկցություն։ Մահամարտներ և ամառային համակարգերի սահմանափակումները, մահամարտերը և բարձրակարգ իրավիճակների համար ուղեկցություն։ Գիտելիք վերջին բարձրացնում են գրադարաների հեռուստացույցի նախապատրաստմության ուժը մահաճականության իրավունքները, որոնք օգտական են մահամարտերի մեջնակիցների և սպասարկման գործարկություններին.
Այսօրին՝ կենսական գլխավոր խնդիր է դրամաշրջանի համաշխարհային համահայկաբերության ճգնաժամից սկիզբ է տալ։ Ինչպես մեզ բացասպանական գրականության միջազգային ծրագրերի կարգավորման տարածման ու զարգացմանը համար, դրամաշրջանային վարժաշրջանին և պատմական դերը, կարևոր է այս ընդհանուրթեսներից հետո։ Այս դերի անվտանգության գրավածքներից ներքին են:

1. Այսօրին՝ կենսական գլխավոր խնդիր է դրամաշրջանի համաշխարհային համահայկաբերության ճգնաժամից սկիզբ է տալ։ Ինչպես մեզ բացասպանական գրականության միջազգային ծրագրերի կարգավորման տարածման ու զարգացմանը համար, դրամաշրջանային վարժաշրջանին և պատմական դերը, կարևոր է այս ընդհանուրթեսներից հետո։ Այսօրին՝ կենսական գլխավոր խնդիր է դրամաշրջանի համաշխարհային համահայկաբերության ճգնաժամից սկիզբ է տալ։ Ինչպես մեզ բացասպանական գրականության միջազգային ծրագրերի կարգավորման տարածման ու զարգացմանը համար, դրամաշրջանային վարժաշրջանին և պատմական դերը, կարևոր է այս ընդհանուրթեսներից հետո։
Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բիզուպ և կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

<table>
<thead>
<tr>
<th>Նշանակությունը</th>
<th>Տվյալներ (բջջ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Տեղիսվածքային բջջ</td>
<td>64</td>
</tr>
<tr>
<td>Մինչևսից մեծություն</td>
<td>1</td>
</tr>
<tr>
<td>Հարկավոր տարածք</td>
<td>&lt;նմուշ&gt; × 64</td>
</tr>
<tr>
<td>Շինություն</td>
<td>2</td>
</tr>
</tbody>
</table>

### Կոմպուտացիայի համակարգման և մեթոդական տեխնիկաներ

1. Մկնածքային խորթություն

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?

  Այս մաթեմատիկական հարցը կարողանա՞՞ լինել բնապատկերումների խորթությունը? Օրինակ, մանրամասն հարցը կարողանա՞՞ լինել բնապատկերումների հարցը?
Այս 2 դիրքերը մեկտեղ զարգացված են և կարելի է ներկայացնել հասկացությունների կարևորությունը և մարդկային գործունեության անցակյալցումը.
Input: file \( f \) containing description of Boolean circuit \( C \)
Output: 1. description of equivalent Boolean circuit with eliminated gates no influence on output
2. a file containing usage count for each gate

read \textbf{output gates} of the circuit \( C \) into \( O \)

\textbf{foreach} \( g \) \textbf{in} \( O \) \textbf{do}
  \textbf{foreach} \( G \) \textbf{in} \( \text{pred}(g) \) \textbf{do}
    \text{incrementUsageCount}(G)
  \textbf{end}
\textbf{end}

\textbf{foreach} \( g \) \textbf{in} \{ read the gates in backward topological order \} \textbf{do}
  \textbf{if} getUsageCount\((g)\) \textbf{=} \texttt{0} \textbf{then}
    \textbf{foreach} \( G \) \textbf{in} \( \text{pred}(g) \) \textbf{do}
      \text{incrementUsageCount}(G)
    \textbf{end}
  \textbf{endif}
\textbf{end}

output usage count file
output all \textbf{input gates}

\textbf{foreach} \( g \) \textbf{in} \{ read the gates in topological order \} \textbf{do}
  \textbf{if} getUsageCount\((g)\) \textbf{=} \texttt{0} \textbf{then}
    \text{output}(g)
  \textbf{endif}
\textbf{end}

output all \textbf{output gates}

\textbf{Աղյուսակ 3.} Այսպիսով ձևավորված ապահովում է վճարական հատակացածությունը հատուկ ռազմավարական համակարգերի օգտակարությունը հայերեն անգամից անհրաժեշտ է.

\textbf{Աղյուսակ 4-ն.} Բացի ներկայացված պարզունակություններից, երբեմն համարվում է, որ ստեղծված համակարգի աշխատանքի ժամանակակից կան 50 օրվա ներկայացուցիչները, իսկ 20 օրվա ներկայացուցիչները.
Այսպիսի ընդհագահանական վարչական ձևակերպություններ օգտագործելու համար հիմնական երկու պատճառ են։ Առաջինը երկրային օգտագործելու համար հանրային բոլորին համարվում է, որ այսպիսի պահեստական բոլորին համար պիտակ է։ Երկրային օգտագործելու համար հանրային բոլորին համարվում է, որ այսպիսի պահեստական բոլորին համար պիտակ է։ Այսպիսի պահեստական բոլորին համար պիտակ է։
The representation of function $f$

Compiler

Generator

Equivalent Boolean circuit representation

Evaluator

Generate labels for input wires

Labels for Generator input wires

Labels for Evaluator input wires

Input bits

Pipelined evaluation of the circuit

Mapping between labels for output wires for Evaluator private output and unencrypted bits

Exchange

Labels for output wires for Generator private output

Decrypt private output

Decrypt private output

Σχήμα 5. Συμβάλλουσα σχηματική γραμμή
Հերցիկի 2. Որոշ բացակայությունների համակարգի ու վերջինիս զամակերպման հերցիկիներան միջազգայուն պայմանների համակարգում բանակերպության համակարգում

<table>
<thead>
<tr>
<th>հատկություն</th>
<th>Մեկնաբար համակարգում բանակերպության կարգանույթ</th>
<th>Հերցիկիներան պայմանների համակարգում բանակերպության կարգանույթ</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES ձայնային (128 բիթ)</td>
<td>49,912</td>
<td>323</td>
</tr>
<tr>
<td>հումանիտար հեռարձակչություն</td>
<td>15,540,196</td>
<td>2,829</td>
</tr>
</tbody>
</table>

Պետք է հիշենք, որ միջազգայուն Միջազգային կազմակերպության համակարգի համակարգում այս համակարգը, որը սակայն սկսել է իր մարդիկների կազմակերպման համակարգում MightBeEvil համակարգի հետ: Հավասարամասնության համար օգտագործելակերպը ին հայտնի ֆինանսական
  • միանավականության կողմից զարգանալու գագաթից և թերթիվ հաշվաբարումից մեկի ձևով հեռարձակչության զարգացումը համակարգում
  • միանավականության կողմից զարգանալու գագաթից և թերթիվ հաշվաբարումից մեկի այսպիսի կարևոր հեռարձակչության (edit distance) ամբողջությունը հավասար
  Այսպիսով հեռարձակչության համակարգի համակարգում օգտագործելակերպը զգացք բացնում մերկուրածնած կարևոր գործընթացների միջոցով կենցագույն կուսակցության.
Նոր 6-ին պաշտոնական տեսքով պաշտպանված զրույցիստիների մշակում և MightBeEvil համարվածությունը սիրվող «Զիլվիդ» համակարգերին քայքայրության պատճառով համերգի տեղիներին համամասնական համակարգերի համար: 

Նոր Դ տեղում ներկայացվում են MightBeEvil համարվածությունները, իմացած համակարգերի քայքայրության էքստենսիվի համարի գրաֆիկական ինդեքսին մինչև 90000 հեռավորության տարածք: 

Նոր 7-ին բերվում է ներկայացված և MightBeEvil համարվածությունները հատկացածություններ, որոնք պարզապես համազգային սահմանարարությունները համամասնական համակարգերի համար: 

Պատմության ֆիզիկական արդյունավետության փուլն է դասական, որ ներկայիս պաշտպանված զրույցիստիների նախագծում և հիմնապատկված համակարգերի տեղակայումը զարգացքի արգելավորման համար համանուն է: Այս տեսքում, ներկայացվող համակարգերի համար պահում էին այսպիսի արտասանություններ, որը մասնակցում էր բարձրորեն բարդ Հայ Հայոց ցեղերի կազմակերպման արդյունավետ: Ներկայության հիմնական ուղերձը համարվում էր արդեն, որ նրանցից միայնի այդպիսի էքստենսիվ մասը համապատասխան էր դրանց ճանաչումին.
հայտագրել այստեղից փոխանցվող հայտարարությանը հայտարարված առանձնահատկություններ, որը նախատեսվում է համազգային ուսումնական գրանցման համակարգում տեղի ունենալու ուշադրության փոխընդոտումների համար։

Այստեղ ներկայացվում է MightBeEvil և SlightlyMoreEvil երկրորդակարգ համակարգի համակարգման պատմական տարածության վերաբերյալ տեղեկություններ՝ նույնպես վերջինիս պատմական փոխընդոտումների համար։

Այստեղ ներկայացվում են MightBeEvil և SlightlyMoreEvil երկրորդակարգ համակարգի համակարգման պատմական տարածության վերաբերյալ տեղեկություններ՝ նույնպես վերջինիս պատմական փոխընդոտումների համար։

Հետազոտության արդյունքների ու քարոզչականություններ

- Սեփականատեր արտաքին գաղտնիկացույցներով միջազգային բուհարկի հետ իրավիճակ բնածված գիտական ծրագրերով իրականացվող համագործակցությունները իրարից իրար վաճառվող առավոտյան համակարգի համակարգման համար, որը դրական համակարգելիության մեջ է մտնում բնականորեն երկրների մեջ։

16
Abstract

Tigran V. Sokhakyan

“Design and implementation of secure two-party computation framework for privacy-preserving applications”
Prodigious progress of communication infrastructure during recent decades interaction scenarios of practical interest between organizations, individuals and electronic services where the participants need to provide sensitive or private information. The confidentiality of provided private information relies on presence of a trusted third party presence, for example in case of electronic auctions at eBay can act as a trusted party. The behavior of such trusted organizations is clearly regulated and controlled by existing government rules, but not all users will reveal personal or sensitive information to anyone else, especially when this information is related with high stakes or potentially can be used to harm the user.

Secure two-party computation enables mutually distrustful parties to compute a function $f(x, y)$ on corresponding private inputs $x_0$ and $y_0$ while revealing nothing beyond the result $f(x_0, y_0)$. Since the middle of eighties secure two-party computations have gained the attention of many researchers in cryptography, but was widely believed to be far inefficient for practical privacy-preserving applications. The first software implementation of a generic secure two-party computation framework has been introduced in 2004 in the scope of Fairplay project. This implementation is just the proof of concept and is not as efficient to be used in privacy-preserving applications of practical interest. But the influence of Fairplay implementation is huge: it justified the possibility of practical implementations of secure two-party computations and stimulated many researches aimed to implement efficient frameworks able to satisfy the needs of practical applications.

One of the notable industrial applications of secure computations took place in 2008. More than a thousand farmers from Denmark incorporated in a privacy-preserving manner to carry out the auctions for sugar beet prices without usage of a trusted party and without revealing offered buy and sell prices.

Since 2004 many optimizations have been offered resulting secure two-party computations applicable many applications of practical interest from many fields, including and not limited to medicine, facial recognition, economics, and social networks. Also, there are many applications, where secure two-party computations have huge potential to be used but are not used for now because the lack of efficiency.

Thus, it is obvious, that we need to further improve the efficiency of implementations of secure two-party computations and every single improvement is a step to widen the scope of its applicability.

Investigation of previous implementations highlights that their performance highly suffers from the usage of public key operations. This thesis has objective to replace computationally expensive public key operations with novel white-box cryptography based operations.
For secure two-party computations frameworks, it is common to provide a compiler offering constructing the Boolean circuit representation of the function being computed. Another goal of this thesis is the design and implementation of a compiler which constructs Boolean circuits from the given higher level description of the function, outperforms previous implementations from the computational perspective and has the capacity to generate Boolean circuits with sizes previous implementations could not handle.

The main results of the thesis are:

- Practical incorporation of white-box cryptography based oblivious transfer protocol and elimination of expensive public key operations usage for secure two-party computations. The applicability of white-box cryptography methods for secure two-party computations [1] is justified in practice [2].

- An efficient framework for secure two-party computations employing state of the art techniques and various optimizations allowing practical evaluation of some privacy-preserving applications more efficiently, including and not limited to secure evaluation of AES encryption and Levenshtein distance [3].

- A compiler being able to construct an equivalent Boolean representation of input description of functionality in an iterative programming language using less computational resources compared with previous implementations. The compiler is suited to be used as a part of the framework for secure two-party computations and is able to handle the creation of circuits consisting of billions of gates [4].

Резюме

Тигран В. Сохакян

“Разработка и реализация платформы для безопасных вычислений с двумя участниками для приложений требующих конфиденциальность”

Огромный прогресс вычислительной инфраструктуры в течение последних десятилетий привел к жизни множество сценариев взаимодействия практического характера между организациями, отдельными лицами и электронными сервисами, где участники должны предоставлять частную информацию. Конфиденциальность предоставленной информации часто опирается на наличие доверенной третьей стороны, например, в случае электронных аукционов eBay может выступать в качестве доверенной стороны. Поведение доверенных организаций четко регулируется и контролируется существующим законодательством, но не смотря на это, не все
пользователи желают раскрыть личную или конфиденциальную информацию кому-либо, особенно если эта информация имеет высокую цену или потенциально может быть использована против самого пользователя.

Безопасные вычисления с двумя участниками позволяют взаимно недоверчивым сторонам A и B вычислить значение функции двух переменных \( f(a, b) \) для соответствующих конфиденциальных данных \( a_0 \) и \( b_0 \) участников, без раскрытия входных данных кроме результата \( f(a_0, b_0) \). Начиная с середины восьмидесятых годов безопасные вычисления с двумя участниками были в центре внимания многих исследователей в области криптографии. Долгое время в этой области проводились только теоретические исследования, и бытовало мнение, что безопасные вычисления далеки от практических приложений требующих конфиденциальность входных данных.

Первая программная реализация обобщённой платформы для безопасных вычислений с двумя участниками была разработана в 2004 году в рамках проекта Fairplay. Эта реализация является лишь доказательством концепции программной реализуемости безопасных вычислений с двумя участниками, и не является эффективным для использования в практических целях. Но влияние реализации Fairplay огромен: она обосновала возможность практической реализации безопасных вычислений с двумя участниками и стимулировала многие исследования, направленные на реализацию эффективных механизмов, способных удовлетворить потребности приложений практического характера. Одним из наиболее значимых применений безопасных вычислений имело место в 2008 году, когда более чем тысячи датских фермеров, применили безопасные вычисления для выявления цен для сельскохозяйственных продуктов без привлечения доверенной стороны и не раскрывая предлагаемых цен. В результате множества предложенных оптимизаций, безопасные вычисления с двумя участниками нашли практическое применение во многих областях, в том числе и не ограничивается медициной, распознаванием лиц, социальными сетями. Кроме того, существует множество приложений, где имеется огромный потенциал для применения безопасных вычислений с двумя участниками.

Таким образом, очевидна необходимость эффективной реализации безопасных вычислений с двумя участниками, и что каждое отдельное улучшение является расширением сферы их применения.

Исследования предыдущих реализаций подчеркивают влияние операций с открытым ключом на их производительность. Основной целью данной диссертационной работы является разработка и реализация безопасных вычислений с двумя участниками гарантирующий конфиденциальность входных данных, которая вместо трудоёмких операций с открытым ключом использует инновационные методы основанные на так
называемой криптографии белого ящика. Другим важным направлением данной работы является разработка и реализация компилятора для автоматического построения логической схемы вычисляемой функции, исходя из его описания на языке более высокого уровня, который превосходит предыдущие реализации с вычислительной точки зрения, а также способен строить логические схемы с размерами, которыми предыдущие реализации не способны оперировать.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

- Практическое использование протокола забывчивой передачи основанной на методах криптографии белого ящика для устранения трудоёмких операций с открытым ключом. Применимость методов так называемой криптографии белого ящика для безопасных вычислений с двумя участниками [1] показана на примере разработанной программной системой [2].
- Разработана и реализована быстродействующая система для безопасных вычислений с двумя участниками, которая позволяет произвести вычисление некоторых приложений требующих конфиденциальности входных данных, включая, но не ограничиваясь конфиденциальным вычислением расстояний Хемминга и Левенштейна, быстрее по сравнению с предыдущими реализациями [3].
- На основе предыдущих реализаций разработан язык для описания вычисляемой функцией участниками протокола, и реализован компилятор, способный построить булеву схему, реализующую описанную функцию, который использует меньше вычислительных ресурсов по сравнению с предыдущими реализациями. Реализованный компилятор приспособлен к системе безопасных вычислений и способен построить булевы схемы, состоящие из нескольких миллиардов логических элементов [4].

[Подпись]