Новокшонов Андрій Костянтинович, науковий співробіт&shy;ник відділу № 165 Міжнародного ННЦ інформаційних техно&shy;логій та систем НАН та МОН України: &laquo;Методи контролю ці&shy;лісності делегованих обчислень&raquo; (01.05.03 - математичне та програмне забезпечення обчислювальних машин і систем). Спецрада Д 26.001.09 у Київському національному універ&shy;ситеті імені Тараса Шевченка

Київський національний університет імені Тараса Шевченка

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Міністерство освіти і науки України

Кваліфікаційна наукова

праця на правах рукопису

НОВОКШОНОВ АНДРІЙ КОСТЯНТИНОВИЧ

УДК 004.05:519.688

ДИСЕРТАЦІЯ

МЕТОДИ КОНТРОЛЮ ЦІЛІСНОСТІ ДЕЛЕГОВАНИХ ОБЧИСЛЕНЬ

01.05.03 – математичне та програмне забезпечення

обчислювальних машин і систем

Подається на здобуття наукового ступеня кандидата фізико-математичних наук

Дисертація містить результати власних досліджень. Використання ідей,

результатів і текстів інших авторів мають посилання на відповідне джерело

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Новокшонов А.К.

Науковий керівник Анісімов Анатолій Васильович, доктор фізикоматематичних наук, професор, член-кореспондент НАН України

Київ – 2020

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ...................................................................... 13

ВСТУП........................................................................................................................ 14

РОЗДІЛ 1. ОГЛЯД ОСНОВНИХ МЕТОДІВ КОНТРОЛЮ ЦІЛІСНОСТІ

ДЕЛЕГОВАНИХ ОБЧИСЛЕНЬ .............................................................................. 20

1.1 Проблема контролю цілісності делегованих обчислень ................................. 20

1.2 Основні підходи з припущеннями щодо можливих збоїв .............................. 24

1.2.1 Методи на основі реплікації обчислень......................................................... 25

1.2.2 Методи на основі аудиту обчислень .............................................................. 27

1.2.3 Методи на основі довіреного обладнання ..................................................... 28

1.2.4 Методи на основі віддаленої атестації........................................................... 30

1.3 Основні підходи без припущень щодо можливих збоїв ................................. 31

1.3.1 Методи на основі імовірнісних систем доведення ....................................... 31

1.3.2 Методи на основі повністю гомоморфного шифрування ............................ 35

1.3.3 Методи для окремих застосувань ................................................................... 38

1.4 Висновки до першого розділу............................................................................ 40

РОЗДІЛ 2. АДИТИВНО ГОМОМОРФНА СХЕМА АВТЕНТИФІКАЦІЇ

ЦІЛОЧИСЕЛЬНИХ ДАНИХ ДОВІЛЬНОЇ ДОВЖИНИ....................................... 42

2.1 Проблема виконання обчислень над автентифікованими даними................. 42

2.2 Побудова схеми ................................................................................................... 48

2.3 Опис алгоритмів схеми....................................................................................... 52

2.4 Аналіз властивостей схеми ................................................................................ 56

2.5 Аналіз складності алгоритмів схеми................................................................. 59

2.6 Висновки до другого розділу ............................................................................. 62

РОЗДІЛ 3. МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ ОБЧИСЛЕНЬ ДЛЯ

ОБМЕЖЕНОЇ ДОДАВАЛЬНОЇ МАШИНИ З ЦІЛОЧИСЕЛЬНИМИ

РЕГІСТРАМИ ДОВІЛЬНОЇ ДОВЖИНИ ............................................................... 63

3.1 Модель обчислень додавальної машини .......................................................... 64

3.2 Загальний опис методу ....................................................................................... 72

3.3 Опис алгоритмів методу ..................................................................................... 77

12

3.4 Аналіз властивостей методу............................................................................... 89

3.5 Аналіз складності алгоритмів методу ............................................................... 94

3.6 Висновки до третього розділу............................................................................ 96

РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМІВ КОНТРОЛЮ

ЦІЛІСНОСТІ ОБЧИСЛЕНЬ..................................................................................... 97

4.1 Опис програмної реалізації ................................................................................ 97

4.2 Приклади програм з перевіркою цілісності обчислень................................. 103

4.3 Експериментальний аналіз швидкодії............................................................. 117

4.4 Порівняння з наявними програмними системами ......................................... 123

4.5 Висновки до четвертого розділу...................................................................... 125

ВИСНОВКИ............................................................................................................. 126

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ............................................................... 127

Додаток 1. Програмний код алгоритмів контролю цілісності обчислень......... 139

Додаток 2. Список опублікованих праць за темою дисертації........................... 148

Додаток 3. Відомості про апробацію результатів дисертації ............................. 149

ВИСНОВКИ

Головнимрезультатомдисертаціїєрозробкасистемиалгоритмівщо

дозволяєконтролюватицілісністьвиконанняделегованихобчисленьнад

цілимичисламидовільноїзаздалегідьнефіксованоїдовжиниЦеробить

суттєвийвнесокврозв’язанняпроблемипідвищеннядовіридорезультатів

такихобчисленьщоєважливимдлягалузірозробкинадійнихобчислювальних

системУроботіотриманотакірезультати

Побудованотапрограмнореалізованоновусхемуавтентифікації

цілочисельнихданихдовільноїдовжиниякадозволяєконтролюватипроцес

виконанняопераційдодаваннятавідніманнянаднимиСформульованоі

доведеновластивостіадитивноїгомоморфностіповнотитакоректності

схемиПроаналізованообчислювальнускладністьалгоритмівсхеми

Розробленоноведлягалузіперевіркицілісностіобчисленьзастосування

моделіобчисленьдодавальноїмашиниякамаєцілочисельнірегістри

довільноїдовжиниПобудованоалгоритмимноженнятаділенняякіможуть

бутиреалізованіуціймоделіобчисленьОсобливістюзастосуванняцієї

моделієвбудованапідтримкаобчисленьнадцілимичисламидовільної

довжинитаможливістьреалізаціїіншихопераційвикористовуючитільки

операціїдодаванняівіднімання

Сформульованотадоведенопрактичноважливіумовицілісностіобчислень

дляконструкційумовнихрозгалуженьтациклівіззаздалегідьне

фіксованоюкількістюітераційякідозволяютьвиявлятинесанкціоновані

модифікаціїпотокукеруваннявалгоритмах

Побудованоалгоритмидляметодуконтролюцілісностіобчисленьнад

цілимичисламидовільноїдовжиниДоведеноповнотутакоректність

методудослідженообчислювальнускладністьйогоалгоритмів

Створенопрограмнийпрототипсистемиконтролюцілісностіобчислень

Результатипроведеногозадопомогоюпрототипуекспериментального

аналізупоказалиможливістьпрактичногозастосуваннярозроблених

алгоритмів