ВІДГУК

офіційного опонента на дисертаційну роботу

Гільгурта Сергія Яковича

«Методи та засоби створення реконфігуровних сигнатурних засобів захисту інформації комп'ютерних систем і мереж»,

подану на здобуття наукового ступеня доктора технічних наук

за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми дисертаційної роботи. Використання програмованих логічних інтегральних схем (ПЛІС) як основи реконфігуровних комп'ютерів та спеціалізованих обчислювачів є сталою тенденцією останніх років. Причому ПЛІС забезпечує оптимальну обчислювальну структуру для різних фрагментів алгоритму або для різних режимів вирішення задачі в залежності від зовнішніх умов.

В дисертаційній роботі, що розглядається, реконфігуровні обчислювачі використовуються для вирішення задач інформаційного захисту за допомогою сигнатурного аналізу. Зовнішніми чинниками для перепрограмування ПЛІС є або поява нових сигнатур для атак, що не були відомі раніше, або зміна умов роботи інформаційної системи, що захищається. Одним із шляхів покращення характеристик такого реконфігуровного обчислювача є комбінування кількох блоків розпізнавання в одному модулі виявлення сигнатур.

Отже, науково-технічна проблема полягає в розвитку методів побудови комбінованих обчислювальних структур для підвищення ефективності сигнатурних технічних засобів захисту інформації, що вирішується в поданій роботі, і вона є актуальною та важливою.

Дослідження з теми дисертації здійснювалося в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України згідно науково-дослідної тематики інституту в рамках відомчих наукових робіт (державна реєстрація № 0114U002361, № 0117U004347) та двох державних конкурсних

програм: Цільова комплексна програма наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань» і Програма інформатизації НАН України (державна реєстрація № 0115U002876, № 0116U006907, № 0118U001370, № 0119U001812).

Ступінь обґрунтованості та достовірність наукових положень, висновків і рекомендацій. Високий рівень обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації обумовлюється коректністю логічного виводу та дотримуванням наукового методу дослідження. Достовірність результатів підтверджується успішними результатами обчислювальних експериментів та досвідом практичного впровадження результатів дослідження.

Наукова новизна результатів дисертації. Наукова новизна результатів автора, та їх співвідношення з відомими раніше положеннями, на думку опонента, виглядає наступним чином.

1. *Вперше* запропоновано метод, який для цифрової схеми, що виконує певну функцію і має відому структуру, дає змогу оцінити апаратні витрати та затримки розповсюдження сигналу при плануванні її реалізації в реконфігуровному обчислювачі, завдяки чому можна швидко виконувати оптимізацію схеми не виконуючи тривалий цикл опису та компіляції схеми засобами САПР. Питома оцінка обчислюється як функція від характеристик реконфігуровного обчислювача та від параметрів заданого набору патернів.

2. Запропоновано *новий* метод спрощення процедури оптимізації цифрової схеми сигнатурного засобу захисту інформації, який полягає у заміні повного перебору всіх варіантів поділу питомого набору патернів між кількома блоками розпізнавання при їх паралельному з'єднанні на сортування патернів, що розпізнаються, за заданою властивістю (довжиною, частотою повторів тощо). Цей евристичний метод дозволяє зменшити часову складність задачі пошуку способу поділу патернів на частини відсортованого списку від

NP-повної (повний перебір) до лінійної, хоча й не гарантує знаходження глобального оптимуму.

3. *Вперше* запропоновано метод проектування модулів сигнатурного аналізу в системах інформаційного захисту на основі відомого принципу розпаралелювання задачі аналізу між паралельними блоками, використовуючи процедуру оптимізації вибору кількості та номенклатури блоків на основі вказаних вище методів швидкої оцінки апаратних та часових характеристик та сортування множини патернів.

4. *Вперше* запропоновано метод проектування модулів сигнатурного аналізу в системах інформаційного захисту на основі відомого принципу розпаралелювання задачі аналізу між послідовно з'єднаними блоками, використовуючи процедуру оптимізації вибору кількості, порядку з'єднання та номенклатури блоків на основі вказаних вище методів швидкої оцінки апаратних та часових характеристик та сортування множини патернів.

5. *Вперше* запропоновано метод проектування модулів сигнатурного аналізу в системах інформаційного захисту на основі відомого принципу розпаралелювання задачі аналізу між кількома блоками, які з'єднані у послідовно-паралельну мережу, використовуючи процедуру оптимізації вибору кількості, порядку з'єднання та номенклатури блоків на основі вказаних вище методів швидкої оцінки апаратних та часових характеристик та сортування множини патернів, а також експертної системи, яка ґрунтується на ідеях різних технічних рішень таких модулів. Причому важливим є балансування апаратних витрат логічних таблиць у одних блоках аналізу, та запам'ятовуючих пристроїв інших блоків, які виконують різні алгоритми.

Повнота викладення результатів дисертації в опублікованих працях. Усі основні результати дисертаційної роботи опубліковані автором в 52 наукових роботах, які відповідають вимогам до опублікування результатів дисертацій, у тому числі: 30 – у наукових фахових журналах та збірниках

наукових праць, з яких 6 – у наукових журналах, що індексуються міжнародними наукометричними базами даних, 21 публікація у працях і матеріалах наукових конференцій.

Автореферат дисертації відображає основні положення дисертаційної роботи, містить дані для його оцінки фахівцями і відповідає вимогам щодо його оформлення.

Значущість дисертаційної роботи для науки і практики

Значущість проведеного дослідження в теоретичному плані полягає в тому, що в ньому розвинути відомі та запропоновані нові методи теорії реконфігуровних обчислень стосовно галузі технічного захисту інформації, а саме, побудови сигнатурних засобів інформаційної безпеки.

Практичне значення роботи обумовлено, по-перше, тим, що нові методи і засоби дають змогу проектувати ефективні системи захисту інформації для комп'ютерних систем і мереж на базі ПЛІС. По-друге, здобуті в четвертому розділі формули для оцінки складності модулів розпізнавання апаратних сигнатурних пристроїв технічного захисту, а також підходи, які використані для цього, можуть бути корисними розробникам відповідних систем. По-третє, створений за участю автора експериментальний зразок веб-сервісу централізованого програмування реконфігуровних обчислювачів на базі хмарної та грід-системи у випадку його повноцінної комерційної реалізації може бути використаний у мережах вітчизняних підприємств та організацій для підвищення їх інформаційної безпеки.

Додатковим свідченням практичної цінності роботи є наведені в роботі акти впровадження результатів дослідження в Національному авіаційному університеті (м. Київ), Київському державному університеті ім. Т.Г. Шевченка (м. Київ), Національному аерокосмічному університеті ім. Н.Є Жуковського "Харківський авіаційний інститут" (м. Харків), та на приватному підприємстві "Геракс" (м. Київ), а також рекомендований лист підтримки від Лундського

університету Швеції, в якому висловлюється висока оцінка розробленого веб-сервісу програмування ПЛІС в грід-інфраструктурі та рекомендується підтримати подальші розробки в даному напрямку в Україні.

Зауваження до дисертаційної роботи. За змістом дисертаційної роботи можна зробити наступні зауваження.

1. В дисертаційній роботі виконано недостатньо широкий огляд алгоритмічно-структурних рішень модулів сигнатурного аналізу, які придатні для реалізації у реконфігуровному комп'ютері. Автор задля швидкої зміни алгоритму аналізу використовує лише властивості внутрішньої пам'яті ПЛІС — влаштовує пам'ять фільтра Блума чи таблицю переходів автомата Ахо–Корасіка у BRAM, вміст якої оперативно оновлюється. Але майже зовсім не розглядається режим динамічної реконфігурації, який мають ПЛІС, що використовуються автором.

Крім того, не прийняті до уваги такі підходи швидкої зміни алгоритмів у системах сигнатурного аналізу на основі скінченного автомату (СА), такі як слабо-детермінований СА (LazyDFA), до якого при потребі динамічно додаються нові стани[1], кістяковий СА (skeleton automata), який конфігурується у ПЛІС як заготовка і стає робочим СА після завантаження в нього умов переходів[2]. Нарешті і фільтр Блума, і автомат Ахо–Корасіка можна ефективно реалізувати апаратно-програмно у конфігурованому мікроконтролері з мінімізованими апаратними витратами зі скороченою програмою, яка завантажується в BRAM[3].

2. Автор стверджує, що використання декількох мікросхем

---

1 Green, T.J., Gupta, A., Miklau, G., Onizuka, M., Suciu, D. : Processing XML streams with deterministic automata and stream indexes. ACM Trans.on Database Systems (TODS), pp. 752–788 (2004).

2J. Teubner, L. Woods, and C. Nie. XLynx—an FPGA-based XML filter for hybrid XQuery processing. ACM TODS, 38(4), December 2013.

3 Sergiyenko, A., Orlova, M., Molchanov, O. Hardware/Software Co-design for XML-Document Processing. /Hu, Z., Petoukhov, S., Dychka, I., He, M. – Ed-s. Advances in Computer Science for Engineering and Education III. 2021. Springer. P. 373-383. DOI 10.1007/978-3-030-55506-1_34

програмованої логіки нераціональне, бо знижує гнучкість та універсальність реконфігуровного обчислювача завдяки фіксованим ("жорстким") з'єднанням між кристалами ПЛІС. Але в контексті його теми це навіть грає роль позитивного фактору, який сприяє динамічному реконфігуруванню, а також безмежному масштабуванню задачі, бо вона відноситься до задач з ідеальним паралелізмом.

3. На думку автора, "конвеєризація додає затримку до поширення сигналу вздовж цифрової схеми на кількість тактів, що дорівнює кількості щаблів конвеєру, тобто підвищує латентність схеми з ростом числа та довжини патернів,...підсилює проблему високого енергоспоживання базової схеми на ЦК". Насправді, саме завдяки конвеєризації можна досягти в ПЛІС максимальних тактових частот і мінімізувати енергію, яка витрачається на виконання алгоритму. Причому конвеєризація у ПЛІС підтримується її архітектурою і фактично не потребує апаратних витрат. Крім того, конвеєризовані модулі компілюються у ПЛІС значно швидше і ефективніше. Такі обчислювачі, як модулі сигнатурного аналізу, як правило, працюють в потоковому режимі без щільних зворотних зв'язків, який підтримується саме конвеєризацією і тому вони не страждають від латентної затримки. У автора, доречі, багато структурних рішень ґрунтуються саме на конвеєризації (затримки різної довжини, послідовне з'єднання блоків).

4. В роботі розглядаються фільтри Блума, які, на думку автора, мають недолік, що довжина патерну має бути фіксованою. Насправді, нічого не перешкоджає використовувати патерни довільної довжини. Більше з тим, автор розглядає можливість рекурсивного розрахунку геш-функції, який, власне, можна припасувати для обробки патернів довільної довжини (шляхом переривання рекурсії наприкінці рядка).

6. В дисертаційній роботі обрано невдалі назви для "Процедури оперативного оновлення", під час якої обов'язково *здійснюється реконфігурація* ПЛІС реконфігуровної сигнатурної системи захисту, для показника

ефективності "Динамічна реконфігурація", яка навпаки полягає у здатності такої системи оновлювати набір сигнатур *без власне виконання реконфігурації* ПЛІС. Назва “щабель” більше пасує до щабля драбинкового фільтра ніж до ступеня конвеєра.

7. В тексті дисертації дублюються позначення для різних змінних, наприклад:

- літерою p позначається як патерн в наборі, так і число портів блокової пам'яті ПЛІС;
- літерою q – внутрішній сигнал в схемі генератора геш-функцій та кількість підсхем часткових фільтрів Блума в складі схеми міні-ФБ;
- літерою Q – показник ефективності пропускної здатності та фрагменти патернів в методі послідовного каскадування;
- та інші.

8. В шостому розділі не наведено графіків чи таблиць, у яких би порівнювались апаратні та часові витрати, які одержані в результаті експериментів та витрати, які розраховані за відповідними формулами, що приведені у четвертому розділі. Таке порівняння необхідне для доведення адекватності моделей, які виражаються цими формулами, справжнім об’єктам.

9. Текст дисертації можна було б скоротити на 10-20% без втрати змісту.

Загальний висновок. У цілому, представлена робота є завершеною науковою працею, виконаною на високому науковому рівні, мета якої досягнута. Наведені зауваження не зменшують її теоретичної та практичної цінності.

За змістом, оформленням, науковими та практичними результатами представлена до захисту дисертаційна робота «Методи та засоби створення реконфігуровних сигнатурних засобів захисту інформації комп'ютерних систем і мереж» відповідає вимогам, що висуваються до докторських дисертацій, а її автор Гільгурт Сергій Якович заслуговує присудження

наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
професор кафедри обчислювальної техніки
Національного технічного університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»,
доктор технічних наук, с.н.с. О.М. Сергієнко