УДК 004.274:004.056

В.Ф. Євдокимов, Київ
А.М. Давиденко, Київ
С.Я. Гільгурт, Київ
О.Р. Ярема, Львів

АПАРАТНА БАЗА РЕКОНФІГУРОВНИХ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Abstract. Recently, a set of combination methods has been proposed aimed at improving the efficiency of reconfigurable security tools by optimizing the synthesis of recognition modules that maximize the benefits of different matching schemes. In this work, we discuss the use of well-known off-the-shelf reconfigurable accelerators (RA) for implementing such methods. Characteristics of real RAs are considered, examples of their use for the techniques of the mentioned methods are given.

Вступ

Розробка методів побудови реконфігуровних засобів захисту інформації, які на відміну від програмних додатків здатні забезпечити в реальному часі розпізнавання сигнатур для таких засобів технічного захисту, як мережеві системи виявлення вторгнень (МСВВ), антивірусні сканери, фільтри протидії мережевим хробакам, тощо, неможлива без аналізу існуючих апаратних пристроїв, на базі яких такі методи планується реалізовувати. На сьогоднішній день виробниками прискорювачів на програмованій логіці пропонується широкий вибір пристроїв, які можуть бути використані в якості реконфігуровних уніфікованих обчислювачів (РУО) [1]. Параметри таких виробів варіюються в широких межах. Отже потенційні споживачі сигнатурних систем технічного захисту можуть мати в експлуатації прискорювачі з дуже різними характеристиками швидкодії, обчислювальної потужності, бортового оперативного запам'ятовуючого пристрою (ОЗП), комунікаційних каналів, та інтерфейсу з хост-комп'ютером. При створенні методів побудови реконфігуровних засобів захисту потрібно враховувати таке розмаїття апаратних пристроїв.

Метою даної роботи є дослідження реконфігуровних засобів. що існують на даний час, які можуть використовуватися в якості РУО при створенні ефективних систем захисту інформації. При цьому головну увагу приділяється аналізу їх технічних показників, що використовуються в новітніх методах побудови оптимальних схем розпізнавання для таких систем.

Побудова ефективних засобів захисту на базі ПЛІС

У роботі [2] на основі аналізу та систематизації світового досвіду конструювання реконфігуровних МСВВ та інших сигнатурних засобів інформаційного захисту запропоновано низку методів підвищення їх

ефективності шляхом синтезу оптимальних структур розпізнавання, які найкращим чином використовують переваги різних підходів щодо побудови таких засобів. Найбільш поширені три напрями, що базуються на наступних технологіях і відповідних технічних рішеннях:

– цифрові компаратори – асоціативна пам'ять;

– хеш-функції – фільтр Блума;

– скінченні автомати – алгоритм Ахо-Корасік.

Особливості кожного з підходів досліджено в роботах [3 – 5].

Як свідчать дослідження, жоден з проаналізованих підходів не демонструє явних переваг перед іншими, кожен має власні позитивні риси та недоліки.

Тому доцільним виглядає намір комбінувати різні підходи в одному пристрої з метою максимізації переваг кожного з них. В результаті формалізації цієї ідеї було запропоновано:

– метод паралельного комбінування (МПрКм);

– метод послідовного каскадування (МПсКс);

– метод вертикального об’єднання (МВрОб).

Підґрунтям методів є той факт, що патерни (фіксовані послідовності символів), які входять до бази даних сигнатур, розрізняються за законом розподілу довжин та властивостями самоподоби, в наслідок чого різні схеми розпізнавання обробляють їх з різною ефективністю. Іншим чинником на користь даних методів є фіксований набір ресурсів реконфігуровних обчислювачів, на базі яких будується система захисту. Використання лише одного способу розпізнавання може призвести до ситуації, коли ресурси, наприклад, логічні використовуються майже повністю, а інші, скажімо, ресурси блокової чи бортової пам'яті – не задіяні взагалі. Як наслідок, максимально можлива ефективність не досягається.

Кожен із запропонованих методів призначений для застосування у відповідних ситуаціях, але в кожному з них шляхом виконання процедур оптимізації обирається з числа можливих способів розподілу патернів між різнорідними блоками такий варіант, для якого досягається екстремум цільової функції за заданим критерієм з урахуванням накладених обмежень. Технічними показниками, найбільш придатними для використання в цільових функціях оптимізації, є ресурсні та часові характеристики [3].

Обов’язковою умовою працездатності згаданих методів є наявність універсальної метрики, що дозволяє оцінювати та порівнювати показники ефективності як окремих блоків розпізнавання, побудованих за різними підходами, так і загального модулю, що скомбінований з них. В якості єдиної вимірювальної одиниці для оцінки ресурсів, що потрібні для синтезу блоків розпізнавання, пропонується використовувати логічний компонент ПЛІС низького рівня деталізації, а саме – пошукову таблицю – lookup table (LUT). При цьому ресурси інших видів зводяться до неї за допомогою нормуючих коефіцієнтів:

$$R_i = L_i + \alpha F_i + \beta B_i + \gamma M_i,$$

де i – номер блоку;

R_i – ресурси, споживані блоком чи модулем розпізнавання;

L_i – ресурси логіки ПЛІС, які потрібні для синтезу i-го блоку (кількість пошукових таблиць LUT);

F_i – ресурси розподіленої пам'яті ПЛІС (кількість тригерів);

B_i – ресурси блочної пам'яті ПЛІС (кількість блоків BRAM);

M_i – ресурси зовнішнього ОЗП – потрібний об'єм бортової пам'яті реконфігуровного обчислювача (Мбайтів);

α, β, γ – коефіцієнти нормалізації ресурсів різного типу стосовно ресурсів логіки (пошукових таблиць LUT).

Обмеження, що накладаються на процес оптимізації, обумовлені скінченністю ресурсів РУО:

$L_{\max}$ – кількість пошукових таблиць LUT у ПЛІС;

$F_{\max}$ – кількість тригерів у ПЛІС;

$B_{\max}$ – кількість блоків BRAM у ПЛІС;

$N_{\max}$ – сумарний об'єм блочної пам'яті ПЛІС (Мбітів);

$M_{\max}$ – об'єм бортової пам'яті реконфігуровного обчислювача (Мбайтів).

Важливою для застосування запропонованих методів є також організація бортової пам'яті (розрядність та число каналів доступу).

Відомо, що при реалізації модулів розпізнавання реконфігуровних засобів патерни фактично "вшиваються" в обчислювальну структуру ПЛІС на апаратному рівні [6]. При виконанні алгоритмів оптимізації згідно запропонованих методів необхідно порівнювати між собою багато варіантів реалізації схеми розпізнавання, для кожного з котрих набір "вшитих" патернів різний. І для кожного з варіантів потрібно розрахувати ресурсні та/або часові витрати. Кожен раз синтезувати схему, наприклад, за допомогою спеціалізованої САПР – непридатне довго. Тому в роботі [2] запропоновано методику прискореного обчислення характеристик блоків, суть якої полягає у створенні для кожного бібліотечного компонента так званої функції-калькулятора. Така функція, маючи на вході заданий набір патернів, обчислює об'єм ресурсів, який потрібен для синтезу блоку, що розпізнаватиме цей набір, а також чисельне значення часової затримки.

Функції-калькулятори для поширених підходів

Нижче наведені приклади функцій-калькуляторів, складених за згаданою методикою для декількох модифікацій відомих підходів до побудови схем розпізнавання.

1. Ресурсна складова функції-калькулятору для ***базової схеми розпізнавання патернів асоціативною пам'яттю на цифрових компараторах BSCAM*** (див. рис. 1, а у роботі [3]) має вигляд:

$$R_{BSCAM} = \sum_{L=m_{\min}}^{m_{\max}} \delta_j \left(\Lambda(x) L + \left\lceil \frac{L-1}{x-1} \right\rceil \right) +$$

$$+ \alpha \left(8 m_{\max} + m_{\min} \left\lceil \frac{\sigma - 1}{y-1} \right\rceil + \sum_{i=m_{\min}+1}^{m_{\max}} \left\lceil \frac{\sum_{L=i}^{m_{\max}} \delta_L - 1}{y-1} \right\rceil \right). \qquad (1)$$

де $\Lambda(\cdot)$ – функція-кваліфікатор, яка визначається як: $\Lambda(z) = \begin{cases} 1, & z \geq 8 \\ 2, & z < 8 \end{cases}$.

У виразі (1) наступні змінні є властивістю вхідної множини патернів:

$m_{\min}$ – довжина найкоротшого патерну;

$m_{\max}$ – довжина найдовшого патерну;

$\delta_j = \delta(j)$ – функція розподілу довжин патернів;

σ – кількість патернів у групі.

Наступні змінні залежать від типу мікросхеми ПЛІС, яка входить до складу РУО, що використовуватиметься:

x – кількість входів пошукових таблиць LUT;

y – здатність навантаження (fan-out) виходів тригерів логічних комірок;

α – коефіцієнт приведення вартості (у сенсі споживання ресурсів) одного тригера до вартості LUT.

2. Ресурсна складова функції-калькулятору для ***спрощеної схеми розпізнавання патернів на базі фільтра Блума (ФБ), що має назву BFs*** (див. рис. 2 у роботі [4]) виглядає наступним чином:

$$R_{\text{BFs}} = \left\lceil \frac{e}{p} \right\rceil \cdot \left(\alpha \cdot \left\lceil \log_2 \frac{e \cdot \delta_L}{\ln 2} \right\rceil + \beta + \left\lceil \frac{\left\lceil \log_2 \frac{e \cdot \delta_L}{\ln 2} \right\rceil}{\left\lfloor \frac{x-1}{2} \right\rfloor} \right\rceil + 4 \right) +$$

$$+ e \cdot \left\lceil \log_2 \frac{e \cdot \delta_L}{\ln 2} \right\rceil \cdot \left(\left\lceil \frac{8L}{x} \right\rceil + (\alpha + 1) \cdot \left\lceil \frac{\left\lceil \frac{8L}{x} \right\rceil - 1}{x-1} \right\rceil - \alpha \right) + \left\lceil \frac{\left\lceil \frac{e}{p} \right\rceil - 1}{x-1} \right\rceil. \qquad (2)$$

Тут змінні, що не залежать від ПЛІС та не були присутні у виразі (1), мають наступний сенс:

e – фактор хибного розпізнавання, який чисельно дорівнює кількості геш-функцій у складі ФБ (є обернено пропорційним до логарифму вірогідності помилки розпізнавання другого роду, яка вважається придатною для конкретного застосування фільтра Блума);

L – довжина патернів, які розпізнаються даним ФБ.

Змінні, які залежать від типу ПЛІС, що входить в РУО:

p – кількість портів блокової пам'яті BRAM;

β – коефіцієнт приведення вартості одного BRAM до вартості LUT.

3. Ресурсна складова функції-калькулятору для ***схеми розпізнавання патернів на базі скінченого автомату Ахо-Корасік (СА-АК) із зовнішньою пам'яттю ACRAM*** (див. рис. 2 у роботі [5]) має вигляд:

$$R_{\text{ACRAM}} = L_{\text{КП}} + L_{\text{КОЗП}} + \alpha\left(F_{\text{КП}} + F_{\text{КОЗП}}\right) + \gamma M_{\text{РУО}}. \qquad (3)$$

Тут:

$L_{\text{КП}}$ і $F_{\text{КП}}$ – кількість відповідно пошукових таблиць LUT і тригерів, що потрібні для створення керуючого пристрою СА-АК;

$L_{\text{КОЗП}}$ і $F_{\text{КОЗП}}$ – кількість відповідно пошукових таблиць LUT і тригерів, що потрібні для створення контролера зовнішньої (бортової) пам’яті РУО;

$M_{\text{РУО}}$ – кількість зовнішньої пам'яті, що потрібна для скінченого автомата.

Змінні $L_{\text{КП}}$, $F_{\text{КП}}$, $L_{\text{КОЗП}}$, $F_{\text{КОЗП}}$ і $M_{\text{РУО}}$ не залежать від ПЛІС і обчислюються за відповідними методиками.

Змінні, які залежать від типу ПЛІС, що входить в РУО:

α – той же коефіцієнт, що і в попередніх прикладах;

γ – коефіцієнт приведення вартості одного Мбайта бортової пам'яті РУО до вартості LUT.

4. Ресурсна складова функції-калькулятору для ***скінченого автомату Ахо-Корасік (СА-АК) із блоковою пам'яттю ACBRAM*** має вигляд:

$$R_{\text{ACBRAM}} = L_{\text{КП}} + r\left(\left\lceil\frac{\lceil\log_2 r\rceil}{x}\right\rceil + 1 + \beta\right) + w\cdot\left\lceil\frac{r-1}{x-1}\right\rceil +$$

$$+\alpha\left(F_{\text{КП}} + w\cdot\left(\left\lceil\frac{r-1}{x-1}\right\rceil - 1\right) + \left\lfloor\log_2\left(M_{\text{BRAM}}/w\right)\right\rfloor\right). \qquad (4)$$

Тут:

$L_{\text{КП}}$ і $F_{\text{КП}}$ –кількість відповідно пошукових таблиць LUT і тригерів, що потрібні для створення керуючого пристрою СА-АК, знайдені також за відповідними методиками;

$r = \left\lceil \dfrac{B}{1024\left(M_{\text{BRAM}} / w\right)} \right\rceil$ – кількість потрібних модулів BRAM,

де B – об'єм потрібної для схеми ACBRAM блокової пам'яті (у Мбітах), який знаходиться як сума об'ємів пам'яті для прямих, перехресних, хибних та післястартових переходів автомата: $B = B_{\text{dr}} + B_{\text{cr}} + B_{\text{fl}} + B_{\text{rs}}$;

w – ширина (розрядність) даних, що зберігаються в BRAM, в бітах (залежить від техніки, яка використовується для побудови скінченного автомату).

Змінні, які залежать від обраної моделі РУО:

M_{BRAM} – об'єм пам'яті (у Кбітах) в одному блоку BRAM ПЛІС (не враховуючі біти парності, якщо вони є);

α, β – ті ж коефіцієнти, що і в попередніх прикладах.

Підсумовуючи наведене, об'єднаємо та перелічимо окремо згадані у виразах (1) – (4) параметри мікросхем ПЛІС та реконфігуровного прискорювача в цілому, значення яких необхідно знати для створення функцій-калькуляторів:

– кількість входів x пошукових таблиць LUT;

– здатність навантаження y виходів логічних комірок;

– кількість p портів блокової пам'яті BRAM;

– об'єм пам'яті M_{BRAM} (у Кбітах) в одному блоку BRAM (не враховуючі біти парності, якщо вони є);

– коефіцієнт α приведення вартості одного тригера до вартості LUT;

– коефіцієнт β приведення вартості одного блока BRAM до LUT;

– коефіцієнт γ приведення вартості одного Мбайта бортової пам'яті РУО до вартості LUT.

Реконфігуровні уніфіковані обчислювачі

На сьогоднішній день у світі виробляється значна кількість пристроїв на базі ПЛІС, які можуть використовуватися в якості реконфігуровних прискорювачів, в тому числі – для вирішення задач інформаційної безпеки. В роботі [7] розглянуто декілька класів подібних приладів, до яких можна віднести як високопродуктивні реконфігуровні обчислювачі універсального призначення, так і менш функціональні, але більш доступні вироби, такі як стартові набори (Starter Kit), тренувальні плати (Trainer Board), оціночні набори (Evaluation Kit), проектні плати (Development Board) та плати-прототипи (Prototype Plate).

Електронний ресурс [8], що налічує більше тисячі найменувань, дає можливість оцінити численність і різноманітність реконфігуровних обчислювачів. Серед найбільш відомих виробників РУО можна назвати такі фірми, як Nallatech [9], Xilinx [10], Alpha Data, National Instruments, DiNI Group та багато інших.

У табл. 1 наведені відомості стосовно низки прикладів реконфігуровних прискорювачів, яка охоплює широкий діапазон пристроїв за технічними характеристиками та функціональними можливостями. Як можна бачити, головні параметри пристроїв, до яких можуть бути застосовані методи МПрКм, МПсКс та МВрОб, відрізняються на декілька порядків.

Таблиця 1

Основні характеристики РУО

Виробник	Nallatech	Nallatech	Xilinx	Digilent	Digilent
Модель	XUP-VV8	385A	VC709 Kit	NetFPGA-1G-CML	Atlys
Клас	РУО	РУО	Evaluation Kit	Development Board	Trainer Board
Тип ПЛІС	Xilinx Virtex UltraScale+ VU13P	Intel (Altera) Arria 10 GX 1150	Xilinx Virtex-7 VX690T	Xilinx Kintex-7 XC7K325T	Xilinx Spartan-6 LX45
Логічних комірок (Cell)	3 780 000	1 150 000	693 120	326 080	43 661
Розмір блоку BRAM, Кбітів	36	20	36	36	18
Об’єм пам'яті BRAM, Мбітів	94,5	54,3	52,9	16,0	2,1
Тип бортового ОЗП	SDRAM DDR4	SDRAM DDR3	SDRAM DDR3	SDRAM DDR3	SDRAM DDR2
Об’єм бортового ОЗП, Гб	512	32	8	0,512	0,128
Мережеві порти, кількість	4x QSFP-DD (2x 100 Gb-Ethernet кожен)	2x QSFP28 (100 Gb-Ethernet кожен)	4x SFP+ (10 Gb-Ethernet кожен)	4x RJ-45 PHY (1 Gb-Ethernet кожен)	1x RJ-45 PHY (1 Gb-Ethernet)
Інтерфейс зв'язку з PC	PCI-Express x16 Gen.3	PCI-Express x8 Gen.3	PCI-Express x8 Gen.3	PCI-Express x16 Gen.2	USB 2.0
Форм-фактор	Dual-slot PCI-E card стандартної висоти 3/4 довжини	Single-slot PCI-E card 1/2 висоти 1/2 довжини	Single-slot PCI-E card стандартної висоти та довжини	Single-slot PCI-E card стандартної висоти 3/4 довжини	Окрема плата 120 x 133 мм
Охолодження	Рідинне	Активне	Пасивне	Відсутнє	Пасивне
Вартість, $	8995	5995	4995	1499	490

Характеристики РУО, що відображені в табл. 1, є типовими параметрами, що містяться у специфікаціях виробів, і якими зазвичай оперують технічні працівники. Але деякі з потрібних для створення функцій-калькуляторів показників, що наведені наприкінці попереднього розділу, є нетиповими. Розробники реконфігуровних сигнатурних апаратних засобів

захисту інформації, які застосовуватимуть згадані вище комбіновані методи, мають докласти додаткових зусиль, щоб їх здобути. (Наприклад, така характеристика, як здатність навантаження (fan-out) виходів логічних комірок, в технічній документації ПЛІС взагалі не наводиться, тому її необхідно знаходити експериментальним шляхом).

Не зовсім простою задачею буває також виявлення максимальних значень деяких параметрів РУО, які потрібні для коректного накладання обмежень на оптимізаційні процедури, що задіяні в комбінованих методах. Перелік характеристик для обмежень наведений на початку попереднього розділу.

В якості пояснення в табл. 2 для тих самих пристроїв, що і в табл. 1, окремо наведені характеристики, які являють інтерес з точки зору використання комбінованих методів, а саме ті, що потрібні для формування функцій-калькуляторів та накладання обмежень.

Таблиця 2

Характеристики РУО, важливі для застосування комбінованих методів

Показник	Познач.	Nallatech	Nallatech	Xilinx	Digilent	Digilent
Модель	-	XUP-VV8	385A	VC709 Kit	NetFPGA-1G-CML	Atlys
Тип ПЛІС	-	Xilinx Virtex UltraScale+ VU13P	Intel Arria 10 GX 1150	Xilinx Virtex-7 VX690T	Xilinx Kintex-7 XC7K325T	Xilinx Spartan-6 LX45
Входів LUT	x	6	8	6	6	6
Кількість портів BRAM	p	2	2	2	2	2
Реальний розмір блоку BRAM, Кбітів	M_{BRAM}	32	20	32	32	16
Кількість LUT	Lmax	1 728 000	427 200	433 200	203 800	27 288
Кількість тригерів	$F_{\max}$	3 456 000	1 708 800	866 400	407 600	54 576
Блоків BRAM	Bmax	2 688	2 713	1 470	445	116
Об’єм пам'яті BRAM, Мбітів (без парності)	$N_{\max}$	86,016	54,260	47,040	14,240	1,856
Бортовий ОЗП: організація, розрядність	$M_{\max}$, організація	4x128 Гб, 64-розр.	2x 16 Гб, 64-розр.	2x 4 Гб, 64-розр.	1x 512 Мб, 32-розр.	1x 128 Мб, 16-розр.

Висновки

В проведеному дослідженні розглянуті аспекти застосування методів (за комбінаційним принципом) підвищення ефективності реконфігуровних

сигнатурних апаратних засобів захисту інформації, які пов'язані з виявленням та використанням специфічних технічних параметрів РУО та мікросхем ПЛІС, на яких вони побудовані. Ці параметри потрібні, по-перше, для складання функцій-калькуляторів, на яких основана методика прискореного обчислення цільових функцій для оптимізаційного процесу, по-друге, для завдання обмежень для цього ж процесу.

Проблеми інформаційної безпеки є актуальними для підприємств та організацій самого різного рівня та розміру. Тому реконфігуровні пристрої, що використовуються в якості апаратних засобів захисту, можуть значно відрізнятися за вартістю та технічними показниками – на кілька десяткових порядків. Тим не менш, згадані методи оптимального комбінування однаково можуть бути застосованими незалежно від абсолютних значень параметрів РУО. Як склад показників, так і спосіб їх використання остаються незмінними для широкого кола реконфігуровних прискорювачі. Цей факт наочно ілюструють приклади виробів, наведені та розглянуті в дослідженні.

1. *Гильгурт С.Я.* Реконфигурируемые вычислители. Аналитический обзор // Электронное моделирование. – 2013. – Т.35, № 4. – С. 49–72.
2. *Гільгурт С.Я.* Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки // Захист інформації. – 2019. – Т. 25, № 2. – С.74-81.
3. *Гільгурт С.Я.* Побудова асоціативної пам'яті на цифрових компараторах реконфігуровними засобами для вирішення задач інформаційної безпеки // Электронное моделирование. – 2019. – Т. 41, № 3. – С.59-80.
4. *Гільгурт С.Я.* Побудова фільтрів Блума реконфігуровними засобами для вирішення задач інформаційної безпеки // Безпека інформації. – 2019. – Т. 35, № 1. – С.53-58.
5. *Гильгурт С.Я.* Побудова скінченних автоматів реконфігуровними засобами для вирішення задач інформаційної безпеки // Захист інформації. – 2019. – Т. 21, № 2. – С.111-120.
6. *Евдокимов В.Ф., Давиденко А.Н., Гильгурт С.Я.* Дополнительные этапы процедуры оперативной реконфигурации аппаратных ускорителей задач информационной безопасности // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2018. – Вип. 85. – С.3-11.
7. *Гильгурт С.Я.* Обзор современных реконфигурируемых унифицированных вычислителей // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2008. – Вип. 49. – С.17-24.
8. FPGA_Boards.shtml [Електронний ресурс]. – Режим доступу: http://www.fpga-faq.com. – Загл. з екрану. – (Дата звернення: 15.09.2019)
9. Bitware. A Molex company [Електронний ресурс]. – Режим доступу: https://www.bittware.com. – Загл. з екрану. – (Дата звернення: 15.09.2019)
10. Xilinx [Електронний ресурс]. – Режим доступу: https://www.xilinx.com. – Загл. з екрану. – (Дата звернення: 15.09.2019)

http://doi.org/10.5281/zenodo.3610626

Поступила 1.08.2019р.