Клієнт і сервер формують сеансовий ключ для подальшого розшифрування даних які вони будуть отримувати один від одного. Сніфер використовуючи відкритий ключ, який він перехоплює під час передачі сертифікату сервером до клієнта, на основі якого створюється попередній та головний секрет (генерація випадкових чисел чи рядків) має змогу отримати дані і про сеансовий ключ. У випадку RSA використовується ключова пара, відкритий та закритий ключ:

Ці ключі зв'язані між собою певним математичним чином, тому знаючи сеансовий ключ клієнта є змога отримати і сеансів ключ сервера. Далі на основі цих ключів і відбувається розбір зашифрованих даних.

Отже, використання сніфер-програм дозволяє здійснити аналіз трафіку, який проходить через мережеву карту. Також програми використовуються адміністраторами для запобігання різного роду проблем які виникають при проходженні даних по мережі. Для збереження своєї інформації потрібно використовувати комутатори та захищені протоколи передачі даних.

Література

1. Пахомов С. Анализаторы сетевых пакетов :[Електронний ресурс] / С. Пахомов. – Режим доступу : http://compress.ru/Archive/CP/2006/4/48.

2. Побегайло А.П. Системное программирование в Windows / А.П. Побегайло. – СПб.: БХВ-Петербург, 2006. – 1056 с.

3. Принцип работы сниффера. Анализаторы трафика : [Електронний ресурс]. – Режим доступу: http://www1.hut.ru/aneksniff/sniffer2.html.

Підхід до функціонального діагностування цифрових процесорів зі скороченою системою команд

Стецюк О.І.
Науковий керівник – к.т.н.,доц. Чешун В.М.
Хмельницький національний університет

Вибір способу саме функціонального діагностування [1] стосовно цифрових процесорів зі скороченою системою команд (ЦПССК) є повністю обґрунтованим з урахуванням внутрішньої складності як ЦПССК об'єктів діагностування, що унеможливлює їх повноцінне тестове детерміноване діагностування та робить малоефективними методи імовірнісного діагностування.

Оскільки основним призначенням ЦПССК є обробка даних, яка виконується програмно-керовано із застосуванням команд з системи команд процесора, то в функціональному діагностуванні процесора можна виділити два основних завдання:

– перевірка здатності діагностуваного ЦПССК коректно виконувати

всі команди з системи команд процесора;

– перевірка здатності діагностуваного ЦПССК коректно виконувати операції з даними, що передбачені кожною застосовуваною командою.

Зрозуміло, що ідеальним варіантом вирішення цих завдань з точки зору повноти діагностичного покриття несправностей ЦПССК є організація його діагностування шляхом перевірки коректності виконання всіх команд з системи команд процесора в різних варіантах їх комбінування (для виявлення можливих взаємозв'язків та взаємовпливів між командами) та з усіма можливими наборами даних.

При зовнішній привабливості такого підходу виникає ряд суттєвих проблем стосовно його застосування:

– загальна кількість елементарних командних перевірок ЦПССК при виконанні всіх його команд в різних комбінаціях та з усіма можливими наборами даних визначається надзвичайно великими комбінаторними числами (навіть з урахуванням того факту, що система команд процесора ідентифікується як скорочена і відрізняється простотою виконання);

– час діагностичних випробувань ЦПССК при реалізації отримуваної кількість елементарних командних перевірок стає також надзвичайно великим і несумісним з допустимими обмеженнями на реалізацію діагностичного експерименту (навіть з урахуванням того факту, що робочі частоти діагностованих процесорів є досить високими і команди характеризуються операційною простотою і, через це, малим часом виконання);

– детально спланувати і проаналізувати хід такого діагностичного експерименту фахівцям майже неможливо навіть із застосуванням для розв'язування типових задач засобів автоматизації з елементами штучного інтелекту.

Зазначені ускладнення "лобової атаки" призводять до потреби розробки оптимізованих методів діагностування ЦПССК [2-5], до числа яких слід віднести методи функціонального діагностування.

При аналізі пропонованого підходу до функціонального діагностування ЦПССК будемо оперувати наступними математичними описами, виконаними із застосуванням інструментарію теорії множин:

– W:{$w1$,$w2$,…,wj,…,wn} – множина функціональних вузлів ЦПССК при його розгляді як об'єкта діагностування;

– K:{$k1$,$k2$,…,kg,…,ks} – множина команд ЦПССК;

– V:{$v1$,$v2$,…, vq,…,vt} – множина елементарних процесорних операцій ЦПССК.

Аналізуючи поставлені завдання перевірки здатності діагностуваного ЦПССК коректно виконувати всі команди $kg \in K$ і, як супутній наслідок, коректно опрацьовувати дані при їх виконанні, та враховуючи архітектурні і функціональні особливості досліджуваних процесорів як об'єктів

діагностування, можна уточнити основні задачі:

– перевірка функціональних вузлів об'єкта діагностування $wj \in W$ на справність;

– перевірка типових елементарних внутрішніх операцій процесора $vt \in V$ на виконуваність.

За суттю, ці два варіанти перевірок є дуже тісно пов'язаними, оскільки перевірка вузлів процесора $wj \in W$ на справність передбачає і реалізується через перевірку типових елементарних внутрішніх операцій процесора $vt \in V$ на виконуваність зазначеними вузлами, але такий розподіл є повністю виправданий з точки зору програмно-керованого (точніше, командно-керованого) функціонального діагностування ЦПССК. Фактично, при командно-керованому функціональному діагностуванні ЦПССК кожна виконувана команда $kg \in K$ залучає в роботу ряд функціональних вузлів процесора $wj \in W$. При цьому команда $kg \in K$ активізує кожен вузол $wj \in W$ на виконання характерної для $kg \in K$ операції $vt \in V$ (сукупності операцій $vt \in V$), що не забезпечує перевірку командою $kg \in K$ всіх операцій $vt \in V$ кожного задіяного вузла $wj \in W$ (наприклад, команда паралельного запису в регістр не перевіряє здатність регістра виконувати операції зсуву). Таким чином, команди $kg \in K$ виконують лише часткові перевірки вузлів $wj \in W$, а для повної їх перевірки необхідно використати певний набір команд з множини K. Реалізація цілеспрямованої перевірки окремого функціонального вузла об'єкта діагностування $wj \in W$ на здатність виконувати всі характерні для нього типові елементарні процесорні операцій $vjt \in V$ дозволить встановити справність саме цього вузла $wj \in W$, але задіюваний для цього набір команд $kg \in K$ одночасно буде задіювати інші вузли процесора $wh \in W$, кожен з яких буде виконувати властиві йому типові елементарні процесорні операції з числа $vhd \in V$. При цьому, практично, абсолютно гарантованим фактом є те, що деякі або всі задіяні вузли $wh \in W$ будуть виконувати не всі характерні для них типові елементарні процесорні операції $vhd \in V$, що не дозволяє говорити про повноцінність виконання перевірок функціонального вузла об'єкта діагностування $wh \in W$ при комплексному виконанні перевірок функціонального вузла $wj \in W$ ($j \neq h$). Оскільки супутні результати, отримувані при виконанні повного комплексу перевірок коректності виконання типових елементарних процесорних операцій $vjt \in V$ функціональним вузлом $wj \in W$, які можна використати для оцінки коректності виконання іншими функціональними вузлами $wh \in W$ ($j \neq h$) хочаб частини характерних для них типових елементарних процесорних операцій $vhd \in V$, ігнорувати недопустимо, виникає потреба відокремленого обліку перевірок функціональних вузлів ЦПССК $wj \in W$ та виконуваних цими вузлами типових елементарних процесорних операцій $vjt \in V$. Це дозволить накопичувати дані про результати перевірок командами $kg \in K$ виконання типових елементарних

процесорних операцій $vjt \in V$ функціональним вузлом $wj \in W$ навіть за умови, що його перевірки будуть виконуватись не систематизовано в часі діагностичного експерименту або як супутні при перевірці інших функціональних вузлів об'єкта діагностування, та фіксувати момент завершення перевірки вузла $wj \in W$ як накопичувальний результат перевірок всіх його типових операцій $vjt \in V$.

Спостережуваність результатів елементарних перевірок при організації функціонального діагностування ЦПССК досягається через відображення характеру впливу реалізовуваних функціональними вузлами $wj \in W$ при виконанні команд $kg \in K$ типових елементарних процесорних операцій $vjt \in V$ над певними заданими наборами даних. При цьому здатність сукупності задіяних функціональних вузлів процесора $wj \in W$ (виконавчих, керуючих і допоміжних) виконувати більшість операцій $vjt \in V$ може бути визначена лише на одному наборі даних (наприклад, для перевірки здатності регістра виконувати операцію зсуву достатньо виконати її на одному двійковому слові даних), а гарантована перевірка коректності виконання функціональним вузлом процесора $wj \in W$ операцій $vjt \in V$ може бути виконана лише при при дослідженні його поведінки на всіх можливих наборах даних або спеціально підібраних оптимізованих наборах даних. Оскільки дослідження поведінки функціональних вузлів об'єкта діагностування на всіх можливих наборах даних є нераціональною, розроблено багато методів формування оптимізованих тестових наборів даних для всіх видів вузлів цифрової електроніки, на більш детальному аналізі розгляді яких зупинятися не будемо.

При визначенні загальних принципів реалізації функціонального діагностування ЦПССК будемо використовувати положення, що перевірка функціональних вузлів $wj \in W$ при реалізації команд $kg \in K$ на здатність виконувати типові процесорні операції $vjt \in V$ зводиться до виконання цих операцій над заданими мінімально-необхідними контрольними наборами даних, а не до виконання повної перевірки для різних наборів даних. Тобто, перевіряється лише здатність виконувати досліджувані операції, а не здатність виконувати ці операції над всіма наборами даних, хоча повна або оптимізована мінімально-достатньо-повна перевірка залишається допустимою за потреби та з використанням інших існуючих методів організації розширених (поглиблених) діагностичних перевірок обраного типу вузлів цифрового процесора.

Визначившись з загальними принципами організації перевірок ЦПССК, слід звернути увагу на порядок організації елементарних командних перевірок об'єкта діагностування (тобто, на принципах визначення пріоритетів щодо використання команд $kg \in K$ в діагностичному експерименті).

Для визначення порядку організації діагностичного експерименту

введемо функцію пріоритету (ваги) команди в діагностичних випробуваннях ЦПССК.

Функція ваги команди $kg \in K$ в діагностичних випробуваннях ЦПССК повинна пов'язуватись зі здатністю команди перевіряти функціональні вузли об'єкта діагностування $wj \in W$ і його типові операції $vt \in V$. Дані щодо здатності команд $kg \in K$ перевіряти функціональні вузли об'єкта діагностування $wj \in W$ і типові операції $vt \in V$ систематизовано в матрицях Pw і Pv відповідно, тому для розрахунку значень функцій пріоритету команд $kg \in K$ використаємо дані цих матриць:

$$F_{k_g \in K} = \alpha_w \sum_{j=1}^{|W|} p(w)_{gj} + \alpha_v \sum_{q=1}^{|V|} p(v)_{gq} , \qquad (1)$$

де $F_{k_g \in K}$ – значення функції пріоритету команди $kg \in K$; αw і αv – вагові коефіцієнти важливості перевірок функціональних вузлів $wj \in W$ і типових елементарних мікрооперацій $vt \in V$ процесора відповідно (задаються апріорно перед початком діагностичного експерименту); $p(w)_{gj}$ і $p(v)_{gq}$ – елементи матриць Pw і Pv відповідно.

Коефіцієнти важливості перевірок вузлів $wj \in W$ і мікрооперацій $vt \in V$ процесора αw і αv дозволяють регулювати надання переваги перевірці саме вузлів $wj \in W$ (збільшуючи значення αw і зменшуючи значення αv) або виконуваних цими вузлами операцій $vt \in V$ (зменшуючи значення αw і збільшуючи значення αv).

За потреби, функцію (1) можна реорганізувати для урахування важливості перевірки кожного функціонального вузла об'єкта діагностування $wj \in W$ і кожної з типових операцій $vt \in V$

Слід зазначити, що можливі два варіанти упорядкування організації діагностичного експерименту на основі значень $F_{k_g \in K}$ функції приоритету команд $kg \in K$.

Перший варіант – з наданням пріоритету при виборі командам $kg \in K$ з мінімальними значеннями $F_{k_g \in K}$ функції приоритету:

$$F_{k_g \in K} \to \min. \qquad (2)$$

При такому підході для організації діагностичного експерименту на основі значень $F_{k_g \in K}$ першочергово будуть обиратися найпростіші команди $kg \in K$, що перевіряють мінімальну кількість функціональних вузлів

$wj \in W$ і типових елементарних мікрооперацій $vt \in V$ процесора, що спростить уточнення місця виникнення несправності при виявленні помилки виконання команди $kg \in K$.

Другий варіант – з наданням пріоритету при виборі командам $kg \in K$ з максимальними значенями $F_{k_g \in K}$ функції приоритету:

$$F_{k_g \in K} \to \max. \tag{3}$$

При такому підході для організації діагностичного експерименту на основі значень $F_{k_g \in K}$ першочергово будуть обиратися найпотужніші команди $kg \in K$, що задіюють максимальну кількість функціональних вузлів $wj \in W$ і типових елементарних мікрооперацій $vt \in V$ процесора. Це прискорить виявлення факту виникнення несправності при виявленні помилки виконання команди $kg \in K$, але ускладнить уточнення місця виникнення несправності (для локалізації місця виникнення несправності знадобиться більше уточнюючих команд).

Виходячи з попередньо проведеного аналізу і зроблених в попередніх розділах висновків можна сформулювати основне положення щодо призначення функціонального діагностування ЦПССК, а також інші базові положення досліджуваного підходу:

1. Мета – перевірити на контрольних наборах даних здатність виконання діагностованим цифровим процесором команд, що утворюють його систему команд, та коректність спрацьовування всіх його вузлів при виконанні характерних для застосовуваних команд елементарних внутрішніх процесорних операцій (мікрооперацій).

2. Підхід базується на принципах командно-керованого функціонального діагностування.

3. Відповідно до двох попередніх положень, основним інструментом організації діагностичних випробувань є команди $kg \in K$, що використовуються для перевірки правильності виконання вузлами процесора $wj \in W$ типових мікрооперацій $vt \in V$ з відображенням результатів діагностичних перевірок на використовуваних контрольних наборах даних.

4. За потреби розширеної перевірки роботи вузлів процесора застосовуються типові процедури тестування вузлів зазначеного класу (в тому числі методи тестового детермінованого або ймовірнісного діагностування [4-8], методи випадкового пошуку [3] тощо).

5. Відбір команд $kg \in K$ для першочергового застосування при перевірці процесора виконується за значенням вагової функції $F_{k_g \in K}$ та у відповідності із заданим критерієм відбору (максимальне або мінімальне

значення $F_{k_g \in K}$ – формули (2) або (3)). Значення функції $F_{k_g \in K}$ обчислюється для команд $kg \in K$ на основі матриць перевірок Pw і Pv за формулою (1).

Література

13. Rayudu K. V. B. V. Functional testing technique for Microprocessor Interface board / K. V. B. V. Rayudu //2015 International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SATA) – P. 1-5

14. Поморова О. В. Метод представлення знань у багатокомпонентних інтелектуальних системах діагностування мікропроцесорних пристроїв / О. В. Поморова, О. Я. Олар // Радіоелектронні і комп. системи. - 2006. - № 6. - С. 110-114.

15. Метод случайного поиска [Електронний ресурс] / Портал «life-prog.ru». – Режим доступу: https://life-prog.ru/1_6778_metod-sluchaynogo-poiska.html (дата звернення 30.10.2018). – Назва з екрана.

16. Тюрин С.Ф. Разработка контрольных и диагностических тестов для КМОП элементов с избыточным базисом / С.Ф. Тюрин, О.А. Громов // Приволжский научный вестник. – Ижевск:ИЦНП, 2013. – № 1. – С.13-21.

17. Глущак Сергій Валеріанович. Метод і засоби тестового діагностування цифрових та мікропроцесорних пристроїв з компонентами, побудованими за КМДН-технологією: Дис. канд. техн. наук: 05.13.05 / Технологічний ун-т Поділля. - Хмельницький, 2002. - 215арк.

18. Кушнєрова Н.І. Вибір та обґрунтування методу тестового діагностування елементів системи попередження нештатних ситуацій на борту повітряного судна / Н.І. Кушнєрова // Системи управління, навігації та зв'язку – Полтава : ПНТУ, 2013. – Вип. 1 (25). – С. 86-89.

19. Шевченко В.В. Визначення технічного стану цифрових типових елементів заміни за допомогою електромагнітного методу діагностування / В.В. Шевченко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 1. – С. 131-135.

20. Кон Е.Л. Подходы к тестовому диагностированию цифровых устройств / Е.Л. Кон, В.И. Фрейман // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь: ПНИПУ, 2012. – № 6. – С. 231-241.

21. Волков Ю.В. Системы технического диагностирования, автоматического управления и защиты: учебное пособие. Часть 1 / Ю.В. Волков – СПб. : ВШТЭ СПбГУПТД., 2016. – 115 с.

22. Дрозд А.В. Вероятностный подход к функциональному диагностированию вычислительных устройств для обработки приближенных данных / А.В. Дрозд // Радіоелектроніка і інформатика. – Харків. : ХНУРЕ, 2004. – № 1. – С. 101-102.