УДК 004.056.53

УСОВЕРШЕНСТВОВАНИЕ АППАРАТНОЙ РЕАЛИЗАЦИИ МЕТОДА АНАЛИЗА АКТИВНОСТИ БЛОКОВ LUT В СОСТАВЕ FPGA-БАЗИРОВАННЫХ СИСТЕМ

К. В. Защелкин[1], А. В. Дрозд[1], Е. Н. Иванова[1], Ю. Ю. Сулима[2]
[1]Одесский национальный политехнический университет
[2]Одесского технического колледжа Одесской национальной академии пищевых технологий

Аннотация. *Рассмотрен подход к обнаружению областей потенциального размещения вредоносных внедрений Hardware Trojans за счет регистрации и анализа активности элементарных блоков LUT FPGA-базированной системы. Выявлен режим функционирования блоков LUT, который не учитывается существующими схемотехническими решениями, обеспечивающими регистрацию активности. Предложены модификации подсхемы регистрации активности блоков LUT, расширяющие ее функционирование на выявленный режим.*

Ключевые слова: *контроль целостности, FPGA, Hardware Trojans, LUT, анализ активности блоков LUT, жизненный цикл FPGA-базированных систем.*

Введение

В номенклатуре элементной базы для построения современных компьютерных систем значительное место занимают программируемые интегральные схемы. Мотивация к использованию интегральных схем такого рода обусловлена возможностью изменения их поведения в динамике жизненного цикла. Наличие этой возможности упрощает отладку, а также устранение ошибок, выявленных на этапе эксплуатации, в устройствах, построенных на основе таких интегральных схем.

При построении компьютерных систем, имеющих высокие показатели производительности, и при этом обладающих гибкостью, обеспечиваемой изменением поведения, обычно используют программируемые логические интегральные схемы (ПЛИС) [1]. Особенностью ПЛИС является высокая степень естественного распараллеливания процесса решения вычислительных задач за счет использования матричной структуры с простыми программируемыми вычислителями в качестве ее элементарных ячеек. Наиболее используемым видом ПЛИС на текущий момент являются микросхемы FPGA (Field Programmable Gate Array) [2].

В контексте информационной безопасности для микросхем FPGA, как для представителей класса программируемых интегральных схем, характерна проблема обеспечения целостности [3] их программного кода. Под целостностью, в данном случае, понимается свойство исключать непредусмотренные изменения системы, возникающие как следствие нелегитимных модификаций ее программного кода.

1. Анализ проблемы и постановка цели работы

Традиционные подходы к контролю целостности программного кода [4], [5] базируются преимущественно на использовании контрольных хэш-сумм [6]. До начала процедуры контроля целостности при помощи выбранной криптографической хэш-функции [7] для программного кода вычисляется хэш-сумма, которая фиксируется в качестве эталонной. После этого в любой момент времени может быть выполнена проверка целостности, которая заключается в повторном вычислении хэш-суммы и сравнении ее с эталонной хэш-суммой. При несовпадении этих хэш-сумм целостность считается нарушенной.

Жизненный цикл FPGA-базированной системы состоит из чередующихся стабильных этапов и этапов модификации системы [8]. В течение стабильных этапов в проект системы или в саму систему не вносятся какие либо изменения, в течение же этапов модификации, проект или система, напротив, подвергаются изменениям. Непредусмотренные (нелегитимные) изменения на стабильных этапах жизненного цикла могут быть выявлены при помощи контроля целостности. На этапах же модификации в систему вносятся легитимные изменения, что требует остановки контроля целостности, пересчета контрольных хэш-сумм и повторного запуска контроля целостности уже с новыми хэш-суммами.

В работе [8] предложен подход к получению информации, дающей возможность локализовать области нарушения целостности, возникающие в результате нелегитимной имплантации в FPGA-базированную систему вредоносных подсхем на этапах модификации наряду с легитимными изменениями системы. Предложенный подход ориентирован на использование для целей поиска

аппаратных закладок (Hardware Trojans) [9], [10] в составе компьютерных систем критического применения [11], для которых характерны два режима функционирования: нормальный и аварийный. Указанный подход заключается во встраивании, в исследуемую на предмет нарушения целостности систему, подсхемы регистрации активности (ПРА) для элементарных вычислительных блоков FPGA – блоков LUT (Look Up Table) [12]. Предлагаемый в работе [8] подход предполагает получение (при помощи указанной встроенной подсхемы) информации о динамике функционирования системы в нормальном режиме. Полученная информация обрабатывается в соответствии с методом, предложенным в работе [8] для локализации возможных областей нарушения целостности.

В работах [13], [14] исследованы возможные варианты аппаратной реализации подхода, представленного в работе [8]. В частности в работах [13], [14] предлагается базовая структура ПРА блоков LUT, образованная совокупностью одинаковых фрагментов, подключаемых к выходам анализируемых блоков LUT. Каждый из фрагментов при этом состоит из двух модулей: а) модуля обнаружения активности, который выдает на свой выход единичный сигнал только в том случае, если имеет место изменение значения на выходе анализируемого подсхемой блока LUT; б) модуля фиксации активности, который фиксирует во внутренней памяти подсхемы факт наличия или отсутствия изменений выходного сигнала блока LUT.

Следует отметить, что схемотехнические решения, представленные в работах [13], [14], не учитывают один из возможных вариантов значений сигналов на выходах блоков LUT в начальный момент функционирования системы. Этот вариант проявляется в виде формирования единичного логического значения на выходе блока LUT в момент начала функционирования системы, в состав которой этот блок входит. Также указанный вариант значений распространяется на случай формирования на выходе блока LUT кратковременного нулевого значения, обусловленного технологическими причинами, за которым следует реальное единичное значение.

Функционирование схемотехнических решений, которое предложены в работах [13], [14], при указанных вариантах входных сигналов, демонстрируют результаты моделирования в среде Intel (Altera) Quartus [15] (рис. 1). На временных диаграммах показаны значения D0, D1, D2, имеющие место на выходах трех анализируемых блоков LUT. Эти значения поступают на входы ПРА блоков LUT. На выходах Q0, Q1, Q2 ПРА формируются результаты регистрации. Выходы блоков LUT, подключенных к входам D0 и D2 подсхемы, в определенные моменты времени меняют свое значение с нулевого на единичное, результатом чего является фиксация активности, которую можно наблюдать в виде единичных значений на выходах Q0 и Q2. Вместе с этим выход блока LUT, который подключен к входу D1 ПРА, имеет константное единичное значение. Отсутствие изменений сигнала D1 должно интерпретироваться (в контексте метода, предложенного в работе [8]) как отсутствие активности блока LUT, подключенного к входу D1. Однако, как видно из результатов моделирования, после снятия единичного значения с входа сброса на выходе Q1 фиксируется активность по входу D1.

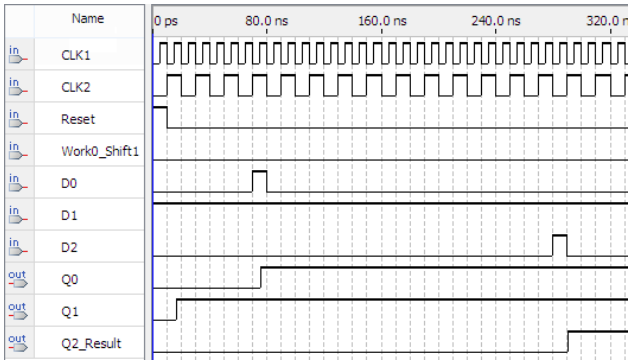

Рис. 1. Результаты моделирования ПРА

Указанные расхождения с теоретически ожидаемыми результатами функционирования ПРА показывают, что решения, представленные в работах [13], [14], не учитывают вариант константного единичного значения на выходе блоков LUT. Исходя из этого, *целью данной работы* является усовершенствование указанных схемотехнических решений для обеспечения корректной обработки единичных значений на выходе блоков LUT в начальный момент работы FPGA-базированной системы.

2. Основная часть работы

Произведен анализ факторов, определяющих причину того, что ПРА, предложенные в работах [13], [14], не учитывают указанные варианты значений на выходах блоков LUT. Установлено, что причиной такого поведения является, различие между значением начального состояния триггеров, входящих в состав модулей обнаружения активности блоков LUT, и значениями на выходах этих блоков.

На рис. 2 в окне схемотехнического редактора САПР Intel (Altera) Quartus показана схема, построенная на основе базовых схемотехнических решений предложенных в работах [13], [14]. Схема предназначена для регистрации активно-

сти трех блоков LUT и состоит из трех фрагментов, каждый из которых включает модуль обнаружения и модуль фиксации активности. Входы D0, D1, D2 (далее D*i*, где *i*=1..3) принимают значения с выходов блоков LUT.

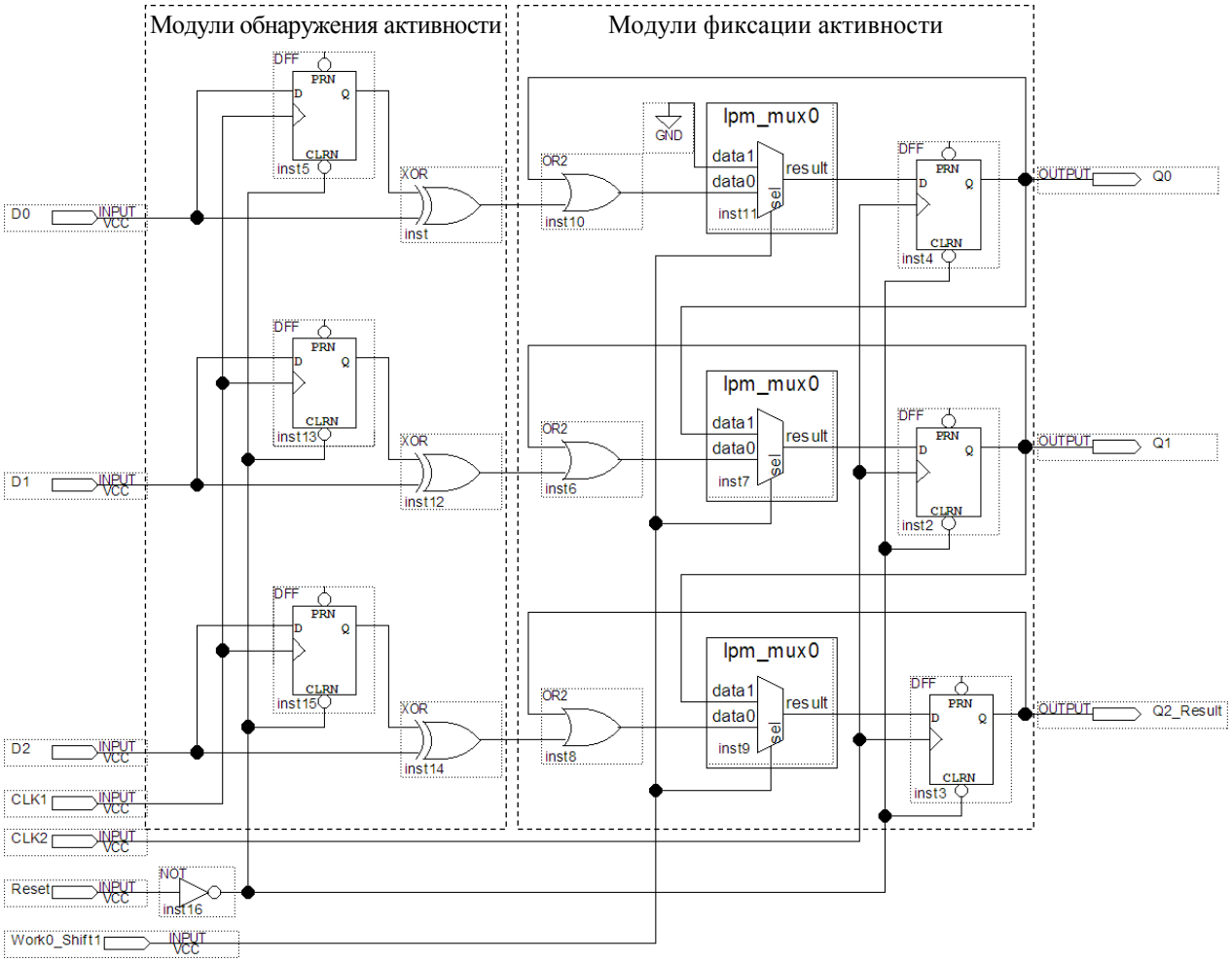

Рис. 2. Анализируемая схема в окне САПР Intel (Altera) Quartus

К каждому из входов D*i* схемы подключен D-триггер и элемент суммирования по модулю 2 (XOR). На вход каждого из элементов XOR поступает текущее значение с выхода блоков LUT и значение, которые имело место на этом выходе на предыдущем такте. На выходах элементов XOR формируются единичные значения (сигнализирующие об обнаружении активности блока LUT) в случае изменения значений на соответствующих входах D*i*.

Описанное выше поведение имеет место только при начальных нулевых значениях на входах D*i*. Если же в начальные моменты времени на входах D*i* присутствуют единичные значения, то на выходах соответствующих элементов XOR сформируется единичное значение при отсутствии изменений значений входов D*i*. Причина такого поведения состоит в нулевом начальном состоянии D-триггеров, подключенных к входам D*i*. В этом случае на один из входов элемента XOR поступает единичное значение с входа D*i* схемы, а на второй вход нулевое значение с выхода триггера, что приводит к формированию единичного значения на выходе элемента XOR и, соответственно, к фиксации активности, которая реально отсутствует.

Предлагается следующий подход к устранению указанного недостатка ПРА. Необходимо обеспечить в начальный момент процесса регистрации активностей совпадение значений, принимаемых с выходов блоков LUT через входы D*i*, с начальным состоянием D-триггеров подключенных к входам D*i*. В рамках указанного подхода предлагается два схемотехнических решения. Первое основано на введении в схему входного сигнала, запускающего процесс регистрации активности, и обеспечивающего запись начального значения с входов D*i* в подключенные к этим входам D-триггера. Второе решение состоит в сбросе триггеров, входящих в состав модулей фиксации активностей, с задержкой относительно входа Reset, что обеспечивает прием корректных результатов обнаружения активностей в эти триггеры.

На рис. 3 показано первое предлагаемое схемотехническое решение – ПРА блоков LUT, в которую введен вход Start и два элемента ИЛИ (OR2): один из них включен в цепь входа CLK1 (выполняющего тактирование процесса обнаружения активностей), второй в цепь входа Reset. В рамках предлагаемого схемотехнического решения начало процесса регистрация активности блоков LUT должно сопровождаться кратковременным единичным импульсом на входе Start.

При переходе сигнала Start из значения 0 в значение 1 выполняется: а) запись текущих значений с входов D*i* в D-триггеры, подключенные к этим входам; б) через входы сброса (CLRN) сбрасываются триггеры, размещенные в модулях фиксации активности. При переходе сигнала Start из значения 1 в значение 0 снимается блокировка изменений состояний триггеров, размещенных в модулях фиксации активности.

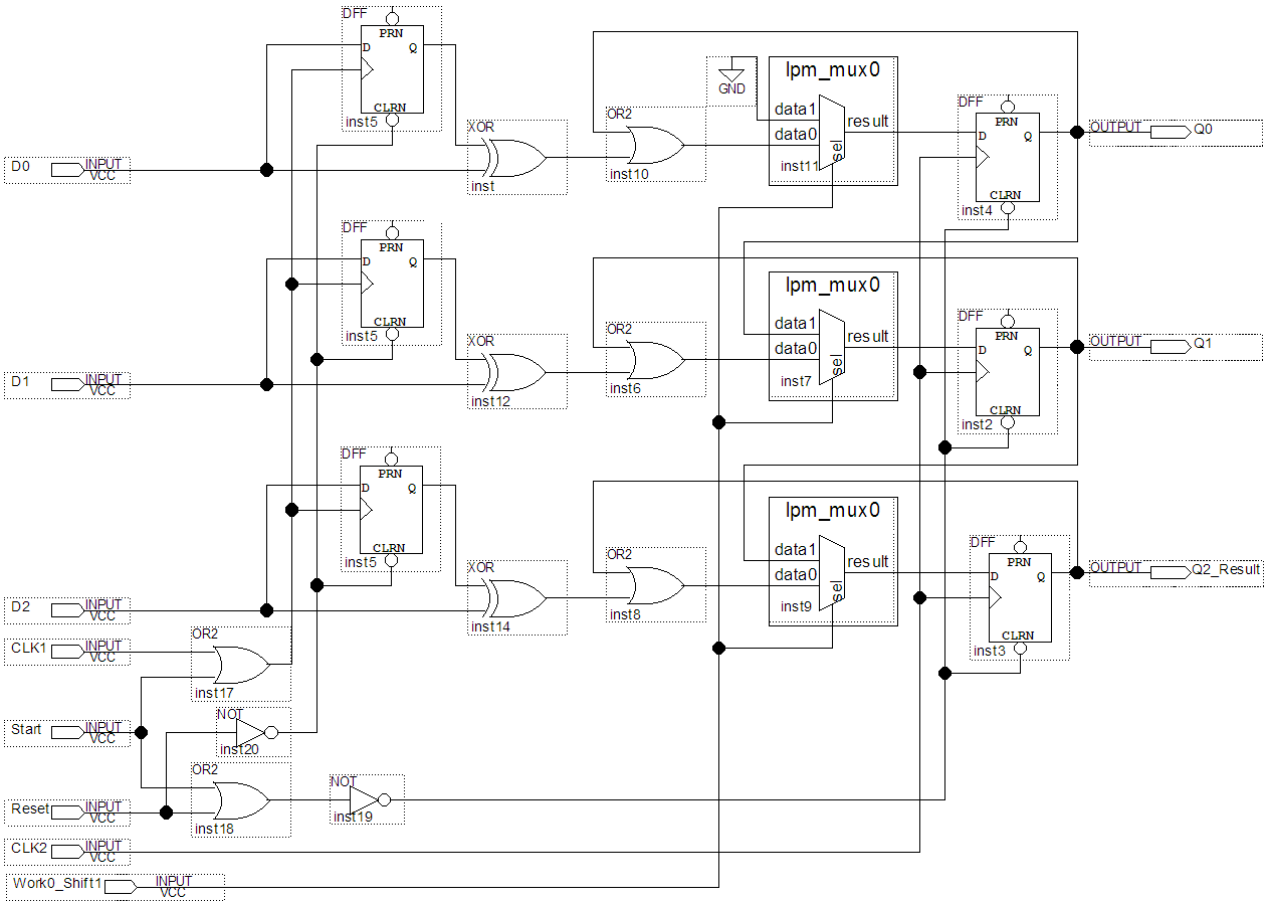

Рис. 3. Модифицированная подсхема с входом запуска регистрации активностей блоков LUT

На рис. 4 показаны результаты моделирования модифицированной подсхемы в среде САПР Intel (Altera) Quartus. Исходные условия моделирования аналогичны тем, которые были показаны на рис. 1. На временной диаграмме видно, что активности по входам D0 и D2 регистрируются так же, как до модификации подсхемы. Отсутствие активности на входе D1, на котором имеет место константное единичное значение, зарегистрировано корректно, т.к. по условию функционирования модифицированной подсхемы начало процесса регистрации совпадает с моментом перехода сигнала Start из значения 1 в значение 0.

На рис 5. показано второе предлагаемое схемотехническое решение. В ПРА введен триггер, который выполняет задержку сигнала, поступающего с входа Reset подсхемы на входы сброса триггеров, расположенных в модулях фиксации активностей.

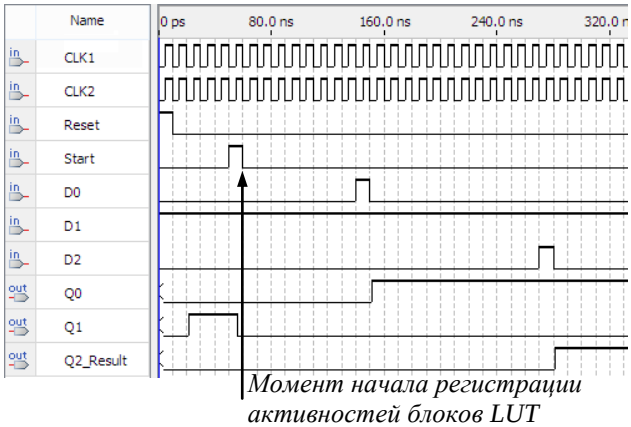

Рис. 4. Результаты моделирования модифицированной подсхемы с входом запуска регистрации

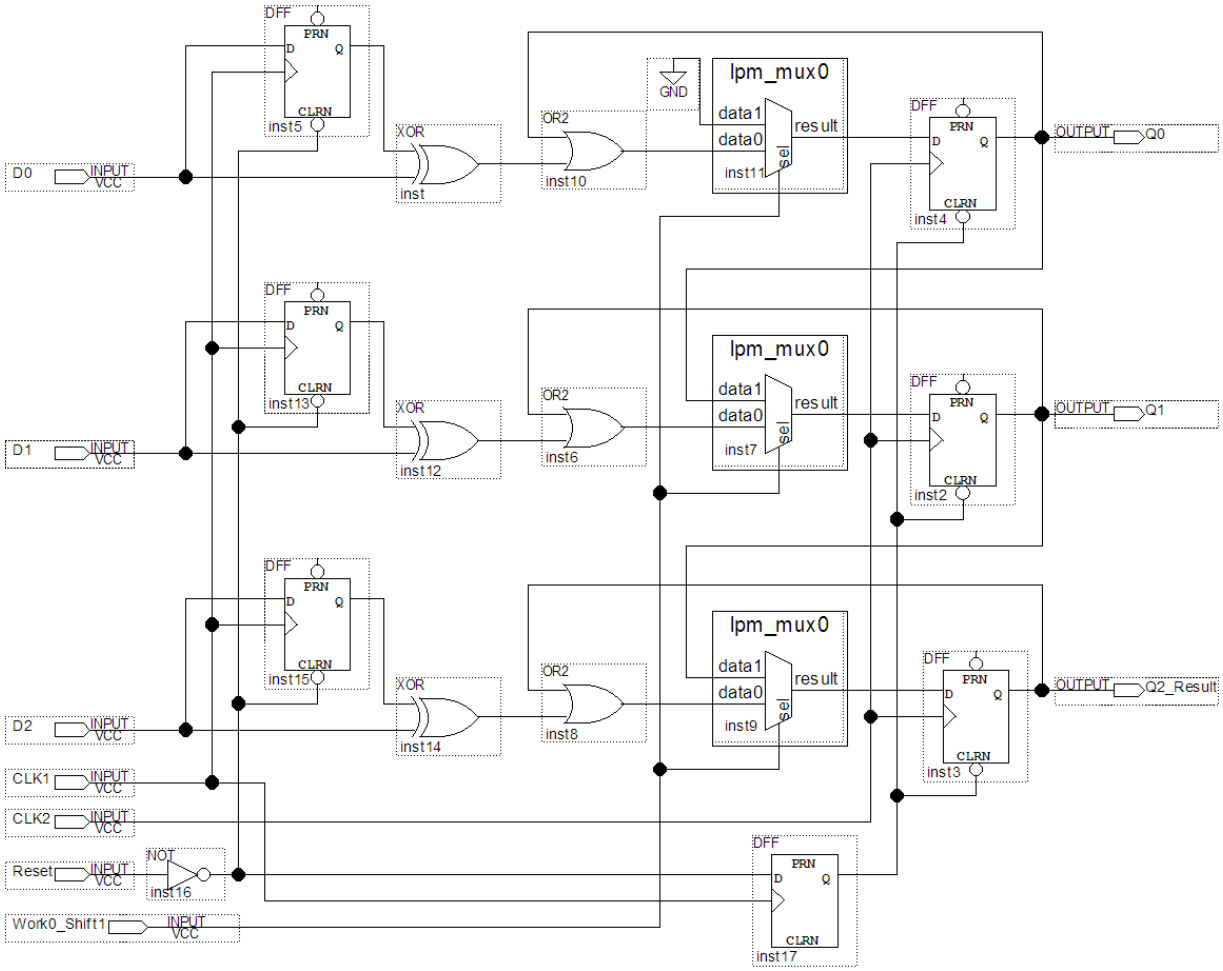

Рис. 5. Модифицированная схема с инициальным сбросом триггеров модулей фиксации активностей

В момент начала функционирования подсхемы, введенный триггер содержит нулевое значение, что обеспечивает сброс триггеров в модулях фиксации активностей, а также блокирует запись в них возможных новых значений. После снятия активного уровня сигнала Reset по тактовому импульсу CLK1, введенный триггер принимает единичное значение и выдает его на свой выход. В результате происходит разблокирование записи новых значений в триггеры модулей фиксации активностей. По этому же тактовому импульсу CLK1 происходит запись текущих значений в триггеры модулей обнаружения активностей, что обеспечивает дальнейшую корректную фиксацию активностей.

На рис. 6 показаны результаты моделирования второго предложенного схемотехнического решений в среде САПР Intel (Altera) Quartus. Исходные условия моделирования аналогичны тем, которые были показаны на рис. 1 и рис 2. Из результатов моделирования видно, что константное единичное значение на входе D1 обрабатывается модифицированной подсхемой корректно, а именно, на выходе Q1 нулевым значением фиксируется отсутствие активности на данном входе.

Предложенные схемотехнические решения позволяют устранить недостатки базовой схемы регистрации активностей блоков LUT. Первое решение позволяет выполнить корректную регистрацию после подачи на его вход специального сигнала запуска регистрации. Второе решение обеспечивает корректную регистрацию активностей в момент начала функционирования подсхемы. В остальном функционирование обеих предложенных модификаций является идентичным.

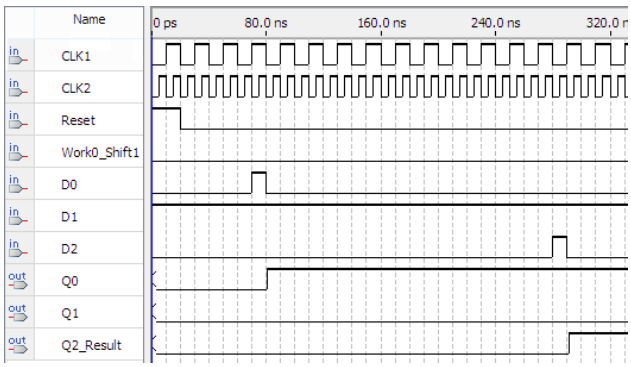

Рис. 6. Результаты моделирования второго схемотехнического решения

3. Выводы

В работе проанализировано функционирование аппаратной реализации метода регистрации активностей блоков LUT. Были выявлены варианты выходных сигналов блоков LUT, которые не учитываются этой аппаратной реализацией. Предложено два схемотехнических решения, позволяющие устранить указанный недостаток. Выполнено моделирование предложенных схем, показывающее их корректное функционирование на множествах входных сигналов, дающих ложную регистрацию активностей при использовании базовой схемы.

Список использованной литературы

1. Sklyarov, V. Synthesis and Optimization of FPGA-Based Systems [Text] / V. Sklyarov, I. Skliarova, A. Barkalov, L. Titarenko. – Berlin: Springer, 2014. – 432 p.

2. Green Experiments with FPGA [Text] / A. Drozd, J. Drozd, S. Antoshchuk, V. Antonyuk, K. Zashcholkin, M. Drozd, O. Titomir // Green IT Engineering: Components, Networks and Systems Implementation / eds. V. Kharchenko, Y. Kondratenko, J. Kacprzyk. – Berlin: Springer International Publishing. – 2017. – Vol. 105, P. 219–239.

3. Bishop, M. Computer Security, 2nd Edition [Text] / M. Bishop. – Boston: Addison-Wesley, 2018. – 1440 p.

4. Katz, J. Digital signatures. Advances in Information Security [Text] / J. Katz. – New York Springer, 2010. – 192 p.

5. Vacca, J. Computer and information security, 2nd edition [Text] / J. Vacca. – USA, Waltham: Morgan Kaufmann Publishers, 2013. – 1280 p.

6. Ferguson, N. Cryptography engineering [Text] / N. Ferguson, B. Schneier, T. Kohno. – USA, Hoboken: Wiley, 2013. – 384 p.

7. Stallings, W. Cryptography and Network Security: Principles and Practice, 7th Edition [Text] / W. Stallings. – United Kingdom, Harlow: Pearson Education Limited, 2017. – 768 p.

8. Zashcholkin, K. The Detection Method of Probable Areas of Hardware Trojans Location in FPGA-based Components of Safety-Critical Systems [Text] / K. Zashcholkin, O. Drozd // Proceedings of IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT-2018. – 2018. – P. 220–225.

9. Tehranipoor, M. Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection [Text] / M. Tehranipoor, H. Salmani, X. Zhang. – Cham: Springer, 2013.

10. Bossuet, L. Foundations of Hardware IP Protection [Text] / L. Bossuet, L. Torres (Eds). – New-York: Springer, 2018. – 248 p.

11. Drozd, A. Features of hidden fault detection in pipeline digital components of safety-related systems [Text] / A. Drozd, M. Drozd, V. Antonyuk // CEUR Workshop Proceedings. – 2015. – Vol. 1356. – pp. 476–485.

12. Vanderbauwhede, W. High-performance computing using FPGAs [Text] / W. Vanderbauwhede, K. Benkrid. – New-York: Springer. – 2016. – 525 p.

13. Защелкин, К. В. Анализ реализации метода регистрации активности блоков LUT в составе FPGA-базированных устройств [Текст] / К. В. Защелкин, А. В. Дрозд // Інформатика та математичні методи в моделюванні. – 2018. – Том 8, № 3. – С. 224–231.

14. Защелкин, К. В. Исследование аппаратной реализации метода регистрации активности блоков LUT в составе FPGA-базированных устройств [Текст] / К. В. Защелкин, А. В. Дрозд // Праці міжнародної наукової конференції "Комп'ютерна алгебра та інформаційні технології, CAIT-2018". – 2018. – С. 105–108.

15. Intel Quartus, [Electronic resource] – Режим доступу: https://www.intel.com/content/www/us/en/software/programmable/quartus-prime/overview.html (дата звернення 24.02.2018).

References

1. Sklyarov, V., Skliarova, I., Barkalov, A. and Titarenko, L. (2014). *Synthesis and Optimization of FPGA-Based Systems*. Springer, Berlin.

2. Drozd, A., Drozd, J., Antoshchuk, S., Antonyuk, V., Zashcholkin, K., Drozd, M. and Titomir, O. (2017). Green Experiments with FPGA, In: V. Kharchenko, Y. Kondratenko and J. Kacprzyk, ed. *Green IT Engineering: Components, Networks and Systems Implementation*, vol. 105. Berlin, Springer International Publishing, pp. 219–239.

3. Bishop M. (2018). *Computer Security, 2nd Edition*. Addison-Wesley, Boston.

4. Katz J. (2010). *Digital signatures. Advances in Information Security*. Springer, New York.

5. Vacca, J. (2013). *Computer and information security*, 2nd edition. MK Publishers, Waltham.

6. Ferguson, N., Schneier, B. and Kohno, T. (2013). *Cryptography engineering*. Wiley, Hoboken.

7. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice, 7th Edition*. Pearson Education Limited, Harlow.

8. Zashcholkin, K. and Drozd, O. (2018). The Detection Method of Probable Areas of Hardware Trojans Location in FPGA-based Components of Safety-Critical Systems. In: *Proc. of IEEE 9th International Conference on Dependable Systems, Services and Technologies DESSERT-2018*, pp. 220–225.

9. Tehranipoor, M., Salmani, H. and Zhang, X. (2013). *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*. Springer, Cham.

10. Bossuet, L. and Torres, L. (2018). *Foundations of Hardware IP Protection*. Springer, New-York.

11. Drozd, A., Drozd, M. and Antonyuk, V. (2015). Features of hidden fault detection in pipeline digital components of safety-related systems. *CEUR Workshop Proceedings*, vol. 1356, pp. 476–485.

12. Vanderbauwhede, W. and Benkrid, K. (2016). *High-performance computing using FPGAs*. Springer, New-York.

13. Zashcholkin, K. and Drozd, O. (2018). The analysis of hardware realization for activeness registration method of LUT units including in FPGA-based devices [Analyz realyzatsyy metoda rehystratsyy aktyvnosty blokov LUT v sostave FPGA-bazyrovannikh ustroystv], *Informatics and mathematical methods in silulation*, Vol. 8, No 3, pp. 224–231.

14. Zashcholkin, K. and Drozd, O. (2018). The Study of Hardware Realization for Activeness Registration Method of LUT Units Including in FPGA-based Devices [Yssledovanye apparatnoy realyzatsyy metoda rehystratsyy aktyvnosty blokov LUT v sostave FPGA-bazyrovannikh ustroystv]. In: *Proceedings of 3th International Conference on Computer Algebra and Information Technologies, CAIT-2018*, pp. 105–108.

15. *Intel Quartus*, [online]. Available at: https://www.intel.com/content/www/us/en/software/programmable/quartus-prime/overview.html [Accessed 24.02.2018].

IMPROVEMENT OF THE HARDWARE IMPLEMENTATION OF METHOD FOR ACTIVITY ANALYSIS OF LUT UNITS IN THE FPGA-BASED SYSTEMS

K. V. Zashcholkin[1], O. V. Drozd[1], O. M. Ivanova[1], J. J. Sulima[2]
[1]Odessa National Polytechnic University
[2]Odessa Technical College of the Odessa National Academy of Food Technologies

Abstract. *The problem of monitoring the integrity of FPGA-based systems program code was considered. It is noted that one of the dangerous types of violation of program code integrity for such systems is malicious implantation of the Hardware Trojans into the system. The approach to the detection of areas of potential location of Hardware Trojans is considered. In the framework of this approach, the detection is performed by registering and analyzing the activity of elementary calculating units LUT of FPGA-based system. The mode of operation of the LUT units, which is not taken into account by the existing circuit solutions that provide registration of the activity, is revealed. This mode is manifested in the form of the formation of a single logical value at the output of the LUT unit at the moment when the system starts functioning. The purpose of the work is to improve the specified circuit solutions to ensure the correct processing of the detected mode of LUT units operation in FPGA-based system. An analysis was made of the factors that cause the existing circuit solutions to function incorrectly under the conditions of the identified mode. It is established that the reason for this behavior is the difference between the value of the initial state of the triggers included in the LUT unit activity detection modules and the values at the outputs of these units. Modifications of the LUT unit activity registration subcircuit are proposed. These modifications expand the correct functioning of the registration subcircuit and correct the incorrect functioning of the existing circuit solutions. The proposed modifications of the subcircuit were simulated. The simulation results showed the correct functioning of the modified subcircuits on the sets of input signals, which give an incorrect registration of activities in the unmodified circuit.*

Keywords: *integrity monitoring, FPGA, Hardware Trojans, LUT, activity analysis of LUT units, life cycle of FPGA-based systems.*

ВДОСКОНАЛЕННЯ АПАРАТНОЇ РЕАЛІЗАЦІЇ МЕТОДУ АНАЛІЗУ АКТИВНОСТІ БЛОКІВ LUT У СКЛАДІ FPGA-БАЗОВАНИХ СИСТЕМ

К. В. Защолкін[1], О. В. Дрозд[1], О. М. Іванова[1], Ю. Ю. Суліма[2]
[1]Одеський національний політехнічний університет
[2]Одеський технічний коледж Одеської національної академії харчових технологій

Анотація. *Розглянуто задачу контролю цілісності програмного коду FPGA-базованих систем. Відзначено, що одним з небезпечних видів порушення цілісності програмного коду таких систем є зловмисні імплантації в систему шкідливих підсхем Hardware Trojans. Розглянуто підхід до пошуку областей потенційного розміщення Hardware Trojans. В межах цього підходу пошук виконується за рахунок реєстрації та аналізу активності елементарних обчислювальних блоків LUT FPGA-базованої системи. Виявлено режим функціонування блоків LUT, який не враховується існуючими схемотехніч-*

ними рішеннями, що забезпечують реєстрацію активності блоків LUT. Цей режим проявляється у вигляді формування одиничного логічного значення на виході блоку LUT в момент початку функціонування системи. Мета роботи полягає в удосконаленні зазначених схемотехнічних рішень для забезпечення коректної обробки виявленого режиму функціонування блоків LUT. Виконано аналіз чинників, які є причиною того, що існуючі схемотехнічні рішення, функціонують некоректно в умовах виявленого режиму. Встановлено, що причиною такої поведінки є відмінність між значенням початкового стану тригерів, що входять до складу модулів виявлення активності блоків LUT, і значеннями на виходах цих блоків. Запропоновано модифікації підсхеми реєстрації активності блоків LUT. Перша модифікація базується на введенні в схему вхідного сигналу, що запускає процес реєстрації активності. Цей сигнал забезпечує запис початкового значення з інформаційних входів схемі в підключені до цих входів тригери. Друга модифікація полягає в скиданні тригерів, що входять до складу модулів фіксації активності, із затримкою щодо входу загального скидання схеми. Виконано моделювання запропонованих модифікацій схем. Моделювання показало коректність функціонування запропонованих в роботі рішень.

Ключові слова: *контроль цілісності, FPGA, Hardware Trojans, LUT, аналіз активності блоків LUT, життєвий цикл FPGA-базованих систем.*

Получено 27.02.2019

Защелкин Константин Вячеславович, кандидат технических наук, доцент кафедры Компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина, E-mail: const-z@te.net.ua, тел.: (048) 734-83-22

Zashcholkin Kostiantyn, PhD, Associate Professor, Department of Computer Intellectual Systems and Networks, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: const-z@te.net.ua, tel.: (048) 734-83-22

ORCID ID: 0000-0003-0427-9005

Дрозд Александр Валентинович, доктор технических наук, профессор кафедры компьютерных интеллектуальных систем и сетей Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина, E-mail: drozd@ukr.net, тел.: (048) 705-83-30.

Alex Drozd, Dr. of Science, Professor, Professor at the Department of Computer Intellectual Systems and Networks, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: drozd@ukr.net, tel.: (048) 705-83-30.

ORCID ID: 0000-0003-2191-6758

Иванова Елена Николаевна, старший преподаватель кафедры Компьютерных систем Одесского национального политехнического университета. Просп. Шевченко, 1, Одесса, Украина, E-mail: enivanova@ukr.net, тел.: (048) 734-83-91

Ivanova Olena, Senior Lecturer, Department of Computer Systems, Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine, E-mail: enivanova@ukr.net, tel.: (048) 734-83-91

ORCID ID: 0000-0002-4743-6931

Сулима Юлиан Юрьевич, кандидат технических наук, заведующий отделением компьютерных систем Одесского технического колледжа Одесской национальной академии пищевых технологий. Ул. Балковская, 54, Одесса, Украина, E-mail: mr_lemur@ukr.net, тел: (048) 732-67-88.

Julian Sulima, PhD, Head of the Computer Systems Department of the Odessa Technical College of the Odessa National Academy of Food Technologies, Balkovskaya st., 54, Odessa, Ukraine, E-mail: mr_lemur@ukr.net, tel: (048) 732-67-88.

ORCID ID: 0000-0003-3986-7296