Для того, чтобы построенное таким образом отношение было отношением сходства, необходимо, чтобы для него выполнялись свойства рефлективности, симметричности и свойства $0 \le \mu_e(IA, IB) + \nu_e(IA, IB) \le 1$.

Лемма 1. Для меры сходства e выполняется свойство рефлексивности, т.е. $\forall IA \in IFS(X)$ $e(IA, IA) = (1,0)$.

Доказательство очевидно, если принять $IB = IA$.

Лемма 2. Для меры сходства e выполняется свойство симметричности, т.е. $e(IA, IB) = e(IB, IA)$.

Доказательство очевидно исходя из свойств операции возведения в квадрат.

Лемма 3. Для меры сходства, полученное по формуле , выполняется свойство $0 \le \mu_e(IA, IB) + \nu_e(IA, IB) \le 1$.

Доказательство.

$$\mu_e(IA, IB) + \nu_e(IA, IB) =$$

$$= 1 - \frac{1}{2n}\sum_{i=1}^{n}\sqrt{(\nu_{IA}(x_i) - \nu_{IB}(x_i))^2 + (\rho_{IA}(x_i) - \rho_{IB}(x_i))^2} + \frac{1}{2n}\sum_{i=1}^{n}\sqrt{(\nu_{IA}(x_i) - \nu_{IB}(x_i))^2} \le$$

$$\le 1 - \frac{1}{2n}\sum_{i=1}^{n}\sqrt{(\nu_{IA}(x_i) - \nu_{IB}(x_i))^2 + (\rho_{IA}(x_i) - \rho_{IB}(x_i))^2} +$$

$$+ \frac{1}{2n}\sum_{i=1}^{n}\sqrt{(\nu_{IA}(x_i) - \nu_{IB}(x_i))^2 + (\rho_{IA}(x_i) - \rho_{IB}(x_i))^2} = 1.$$

Так как $\sqrt{a^2 + b^2} \le |a| + |b|$, получаем

$$\mu_e(IA, IB) + \nu_e(IA, IB) \ge$$

$$\ge 1 - \frac{1}{2n}\sum_{i=1}^{n}|\nu_{IA}(x_i) - \nu_{IB}(x_i)| - \frac{1}{2n}\sum_{i=1}^{n}|\rho_{IA}(x_i) - \rho_{IB}(x_i))| + \frac{1}{2n}\sum_{i=1}^{n}|\nu_{IA}(x_i) - \nu_{IB}(x_i)| =$$

$$= 1 - \frac{1}{2n}\sum_{i=1}^{n}|\rho_{IA}(x_i) - \rho_{IB}(x_i))| \ge 0.$$

Таким образом леммы 1-3 показывают, что отношение, определенное функцией e является корректно построенным интуиционистским нечетким отношением сходства и поэтому может быть использовано при кластеризации данных, представленных интуиционистскими нечеткими множествами.

Список использованных источников:

1. Atanassov K. On Intuitionistic Fuzzy Sets Theory / K. Atanassov. – Springer-Verlag, 2012. – 323 p.
2. Кофман А. Введение в теорию нечетких множеств / А. Кофман. – М.: Радио и связь, 1982. – 432 с.
3. Szmidt E. Distances and Similarities in Intuitionistic Fuzzy Sets / E. Szmidt. – Springer-Verlag, 2014 – 148 p.
4. Wang Z. A netting clustering analysis method under intuitionistic fuzzy environment / Z. Wang [et. Al]. // Applied Soft Computing. – 2011 - №8. – p. 5558–5564

МЕТОДИКА ЗАМЕНЫ КЛЮЧА ДЛЯ СХЕМЫ АКТИВНОГО ИЗМЕРЕНИЯ ЦИФРОВЫХ УСТРОЙСТВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Заливако С.С.

Иванюк А. А. – д-р. техн. наук, доцент

В работе рассмотрена модификация существующей схемы активного измерения с помощью логически реконфигурируемой физически неклонируемой функции, в результате изменения состояния которой появится необходимость в замене ключа. Реализация изменений в цифровом конечном автомате может быть осуществлена по средствам его реконфигурирования или же кодирования определенного небольшого числа возможных изменений ключа в структуре конечного автомата.

В настоящее время на рынке интегральных схем (ИС) наблюдается тенденция роста количества компаний (с 7 % в 2000 году до 30 % сейчас), которые передают свои проекты для изготовления крупным корпорациям, владеющим современными производственными мощностями [1]. Существующее законодательство не всегда способно защитить компании, проектирующие ИС, от перепроизводства продукции по их проектам. В связи с этим возникает необходимость в защите проектных описаний, права интеллектуальной собственности на которые принадлежат компаниям, не имеющим своих производственных мощностей.

Одним из возможных подходов является активное измерение ИС и, в частности, цифровых устройств (ЦУ). Под *активным измерением* ЦУ понимают такие протоколы безопасности, которые позволяют владельцу прав интеллектуальной собственности на проектное описание осуществлять контроль над ЦУ, произведенными по этому описанию. В свою очередь, контроль осуществляется не только по информации, уникально идентифицирующей ЦУ, но и внедрением возможности активации и деактивации ЦУ после его производства.

Рассмотрим один из существующих методов активного измерения [2]. На первом этапе проектировщик ЦУ разрабатывает высокоуровневое проектное описание. Далее необходимо извлечь из проектного описания структуру цифрового конченого автомата (ЦКА) и расширить ее за счет дублирования некоторых состояний и добавления фиктивных переходов между ними. В результате чего будет получен расширенный ЦКА (РЦКА) устройства, который изначально находится в неактивном состоянии, поскольку производителю неизвестна его структура. Также на этапе проектирования ЦУ осуществляется внедрение физически неклонируемой функции (ФНФ) для генерирования уникальных пар запросов и ответов, которые кодируют состояния и переходы между ними.

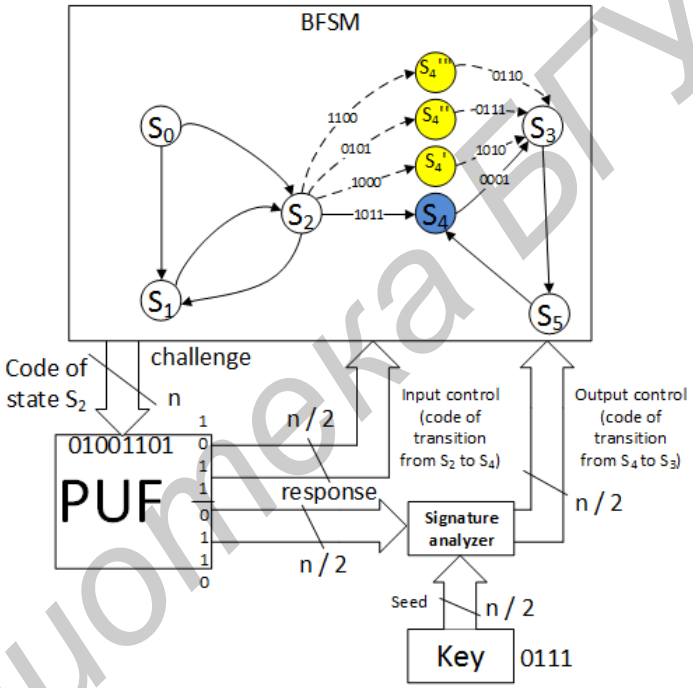

Рис. 1 – Схема активного измерения ЦУ

Рассмотрим алгоритм работы описанной выше схемы (см. Рисунок 1). Запрос к ФНФ одновременно является и кодом состояния в РЦКА. По этому запросу от ФНФ можно получить ответ, который делится на две равные части: первая кодирует выходной переход из состояния, а вторая является основой для генерирования кода выходного перехода. Для вычисления кода выходного перехода используется сигнатурный анализатор, начальным значением для которого является ключ, который используется для активации ЦУ.

Недостатком такой схемы является то, что пары запросов и ответов хотя и уникальны для каждого ЦУ, но не могут быть изменены со временем и таким образом, делают невозможной замену ключа.

Для замены ключа предлагается использовать логически реконфигурируемую ФНФ (ЛР-ФНФ) [3]. Процесс генерирования информации о состоянии ЛР-ФНФ может быть реализован с помощью линейного сдвигового регистра с обратной связью (англ. Linear feedback shift register (LFSR)). Процесс замены ключа схематически изображен на Рисунке 2.

На первом этапе происходит изменение состояния LFSR, встроенного в ЦУ. В результате чего изменяется состояние ЛР-ФНФ и, соответственно, изменяются пары запросов и ответов, что влечет за собой некорректность кодов выходных переходов, вычисленных на основе текущего ключа.

На втором этапе пользователь запрашивает новый ключ, поскольку ЦУ оказалось в неактивном состоянии в результате изменения состояния ЛР-ФНФ.

На третьем этапе владелец прав интеллектуальной собственности на проект ЦУ, зная информацию о запросах и ответах ЛР-ФНФ в текущем состоянии, вычисляет новое значение ключа, которое сможет активировать ЦУ.

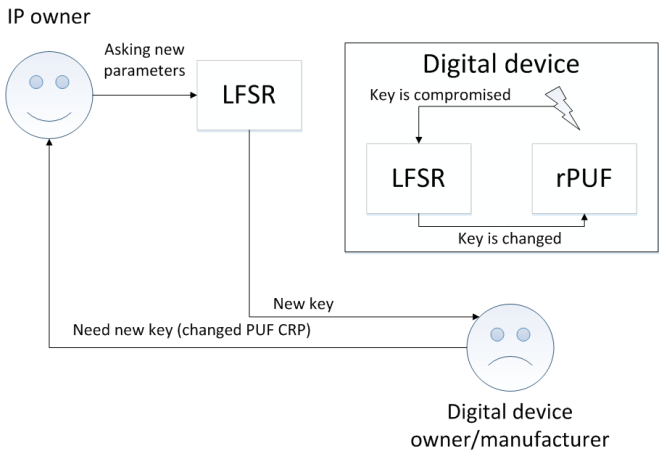

Рис. 2 – Замена ключа в предлагаемой схеме активного измерения

Проблемой на данном этапе является реализация изменения конечного автомата ЦУ без повторного синтеза проекта. Поскольку все состояния и переходы закодированы в РЦКА, то их изменение возможно только в результате повторного кодирования состояний и переходов и, соответственно, синтеза нового проекта, что является недопустимым в схеме активного измерения.

В связи с этим предлагается два подхода для решения этой проблемы:

1. Предположение о том, что изменений ключа будет немного. Например, ключ может изменяться не более чем *k* раз за все время использование данного устройства, где *k* – некоторое целое число, не превышающее 10. Таким образом, на первом этапе разработчику проекта ЦУ необходимо для всех возможных *k* состояний собрать информацию о запросах и ответах ЛР-ФНФ. Таким образом, кодирование основных состояний не изменится, а при их дублировании необходимо задать такие переходы, которые соответствуют каждому из *k* состояний ЛР-ФНФ. В целях улучшения безопасности возможно дублирования каждого из состояний не только *k* раз для работоспособности, но и большего числа раз (т.е. создание фиктивных состояний, которые не имеют отношения к парам запросов и ответов ЛР-ФНФ). Такой подход позволит решить проблему замены ключа, однако он не является гибким по отношению к количеству замен ключа, поскольку увеличение числа *k* повлечет за собой значительное увеличение аппаратурных затрат;
2. Изменение структуры конечного автомата, которое может позволить осуществлять реконфигурацию. Например, возможно использование иерархических ЦКА [4].

Предложена методика замены ключа для существующей схемы активного измерения. Решение данной проблемы позволит осуществлять удаленный контроль над цифровым устройством после его производства, поскольку предоставляет возможность замены ключа с помощью изменения состояния встроенного LFSR. Главным недостатком приведенной методики является значительное увеличение аппаратурных затрат в случае использования предположения о малом количестве возможных замен ключа.

Список использованных источников:

1. Clarke, P. Fabless Chip Companies Ranked by 2013 Sales [Electronic resource]. – UBM Tech, 2013. – Mode of access: http://www.eetimes.com/document.asp?doc_id=1322324&page_number=2. – Date of access: 10.03.2015.
2. Alkabani, Y., Koushanfar, F., Potkonjak, M. Remote activation of ICs for piracy prevention and digital right management // Computer-Aided Design, ICCAD. – 2007. – p. 674 – 677.
3. Kursawe, K. Recon_gurable physical unclonable functions enabling technology for tamper-resistant storage / K. Kursawe, A.-R. Sadeghi, B. Scoric, P. Tuyls // Hardware-Oriented Security and Trust (HOST), San Francisco, USA, July 27, 2009. – New York: IEEE, 2009. – p. 22 – 29.
4. Lee, S., Yoo, S., Choi, K. Reconfigurable SoC design with hierarchical FSM and synchronous dataflow model // Hardware/Software Codesign, CODES. – 2002. – p. 199 – 204.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ BIG DATA В ВЕБ-АНАЛИТИКЕ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кушмар С. Е.

Пилецкий И. И. – канд. физ.-мат. наук, доцент

Активно развивающиеся технологии Big Data позволяют анализировать новые источники данных, которые совсем недавно были недоступны ввиду их значительного объема, большой скорости поступления и невозможности традиционной структуризации. В настоящее время до 80% данных – это неструктурированные данные. В веб-аналитике