АППАРАТНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ИДЕНТИФИКАЦИИ ПЛИС НА ОСНОВЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: ivaniuk@bsuir.by

В докладе рассматривается аппаратная реализация алгоритма идентификации цифровых устройств на основе физически неклонируемых функций (ФНФ). Решается задача уменьшения выработки нечетких ответов ФНФ путем многократной подачи множества запросов и мажоритарного подсчета соответствующих им ответов. Множество стабилизированных ответов при этом предлагается сжимать посредством метода адаптивного сигнатурного анализа (АСА). Значение результирующей сигнатуры можно использовать в качестве уникального неклонируемого идентификатора цифрового устройства.

Введение

Среди всего многообразия методов и средств защиты цифровых устройств и систем от несанкционированного использования особо выделяют методы идентификации и аутентификации, при реализации которых в последнее время все чаще применяют так называемые физически неклонируемые функции (ФНФ). По одному из определений [1] ФНФ является характеристика физической (цифровой) системы, которая не подлежит клонированию на других системах. Аппаратная реализация ФНФ представляет собой цифровую схему, имеющую n входов, на которые подаются двоичные значения из множества запросов C (Challenge), и один выход, обеспечивающий появление двоичного символа из множества ответов R (Response). Каждому запросу $c_i \in C$ ($i \in \{0, ..., 2^n - 1\}$) соответствует уникальное значение $r_i \in \{0, 1\}$, при этом множество пар $CR = \{(c_0, r_0), (c_1, r_1), ..., (c_{2^n-1}, r_{2^n-1})\}$ и есть уникальная неклонируемая характеристика схемы. Обладая информацией об одной паре (c_i, r_i) нет никакой возможности рассчитать, смоделировать либо другим способом предсказать значение пары (c_j, r_j), $i \neq j$, или другое множество пар. Для цифровых устройств идея реализации ФНФ основана на использовании физических вариаций технологического процесса изготовления интегральных схем. Такие вариации носят случайный характер и не могут быть предсказаны, а тем более клонированы.

Свойства цифровых ФНФ позволяют решать такие задачи как, реализация неклонируемых идентификаторов и надежных механизмов аутентификации, защита от нелегального копирования (клонирования) цифровых систем, построение генераторов случайных невоспроизводимых последовательностей и аппаратных хэш-функций.

В данной работе рассматривается один из вариантов аппаратной реализации алгоритма идентификации с использованием ФНФ, который формально можно представить как получение значения уникального идентификатора id из множества CR.

I. Применение ФНФ для идентификации

Идентификация цифровых устройств организовывается различными способами:

- реализация неперезаписываемого регистра идентификатора на эта производства;
- реализация однократно программируемого регистра идентификатора;
- реализация многократно программируемого регистра идентификатора.

Инициализированное значение регистра идентификатора может быть использовано для адресации цифрового устройства, подключенного к системной шине, для генерирования секретного ключа при реализации протоколов аутентификации и алгоритмов шифрования и т.п. Большинство программируемых логических интегральных схем (ПЛИС), особенно мало бюджетных, не имеют аппаратных средств идентификации, что заставляет разработчиков собственными средствами решать данную проблему на уровне исходных проектных описаний цифровых устройств. При этом значение идентификатора становится легкодоступным со стороны злоумышленников, которые могут несанкционированно его изменять либо клонировать.

Реализацию k-разрядного двоичного идентификатора id на основе ФНФ можно описать при помощи следующего оператора: $A(CR^*) = id$, где $CR^* \subseteq CR$, при этом $k \ll 2^n - 1$. Для сокрытия механизма ФНФ от атак извне можно использовать следующую схему идентификации цифрового устройства (см. рис. 1).

Однобитный запрос *request* инициирует алгоритм извлечения уникальной структурной информации ФНФ путем получения подмножества CR^* с последующим его преобразованием в значение id.

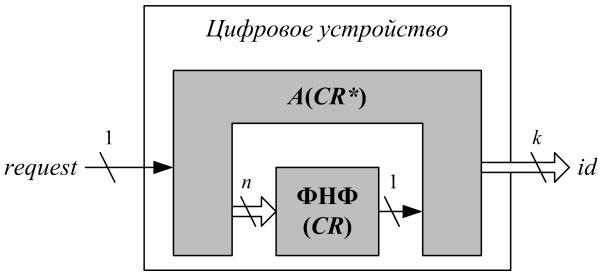

Рис. 1 – Обобщенная схема идентификации

Основной проблемой практической реализации данного подхода является эффект нестабильности ответов при многократном применении одних и тех же значений запросов. Пара (c_i, r_i) называется парой с нечетким ответом, если $P_i^t(c_i, r_i) = \sum_{l=1}^{t} \frac{r_i}{t} \in]0,1[, \forall t > 1$, где t – число независимых экспериментов по извлечению ответа r_i на один и тот же запрос c_i. Другими словами значение $P_i^t(c_i, r_i) = P_i^t$ может быть интерпретировано в качестве вероятности появления единичного ответа $r_i = 1$ при повторении t раз запроса c_i. Если $P_i^t \in \{0,1\}, \forall t > 1$, то пара (c_i, r_i) называется стабильной парой на t экспериментах. Например, для ФНФ типа арбитр [2] с протяженностью симметричных путей равной 8 и реализованной на FPGA SPARTAN-3E пара с номером $i = 3$ является стабильной ($P_3^3 = P_3^7 = P_3^{15} = ... = P_3^{255} = 0$), а нулевая пара ($i = 0$) является парой с нечетким ответом ($P_0^3 = 1.0$, $P_0^7 = 0.85$, $P_0^{15} = 1.0$, ..., $P_0^{255} = 0.97$). Пусть множество $GS^t = \{P_0^t, P_1^t, ..., P_{m-1}^t\}$, $m \leq 2^n$. Очевидно, на основе приведенного примера, $GS^3 \neq GS^7 \neq GS^{255}$, что затрудняет процесс идентификации. На основе множества GS^t получим новое множество $BW^t = \{B_0^t, B_1^t, ..., B_{m-1}^t\}$, элементы которого $\forall i = \overline{0, m-1}, t = 2 \cdot j + 1, j = 1, 2, 3, ...$ будут формироваться следующим образом:

$$BW_i^t = \begin{cases} 0, & \text{если } P_i^t < 0.5; \\ 1, & \text{если } P_i^t \geq 0.5. \end{cases} \quad (1)$$

Проведенные исследования для описанного выше типа ФНФ дают следующие результаты: $BW^3 \neq BW^7 \neq BW^{15} = BW^{31} = ... = BW^{255}$. Полученная стабильность бинарных множеств BW^t для $t \geq 15$ позволяет на их основе формировать значение идентификатора. Для сжатия множества BW^t предлагается использовать адаптивный сигнатурный анализ (АСА) [3], являющийся разновидностью методов сжатия с потерей данных. Согласно АСА значение идентификатора вычисляется следующим образом:

$$id = \bigoplus_{i=0}^{m-1} i, \forall BW_i^t = 1, \quad (2)$$

где $\bigoplus$ есть операция поразрядной суммы по модулю два двоичного представления индекса i. Таким образом разрядность id составляет $k = \lceil log_2 m \rceil \ll 2^n - 1$ бит. При этом алгоритм формирования id можно представить последовательным преобразованием рассмотренных множеств: $CR^* \Rightarrow GS^t \Rightarrow BW^t \Rightarrow id$.

II. Аппаратная реализация

Аппаратная реализация предложенного алгоритма идентификации была произведена при помощи платы быстрого прототипирования Digilent Nexys-2 [4], в состав которой входит FPGA SPARTAN-3E. За основу схемной реализации ФНФ была взята ФНФ типа арбитр с фиксированной длиной симметричных путей. Обобщенная структура схемы идентификации представлена на рисунке 2.

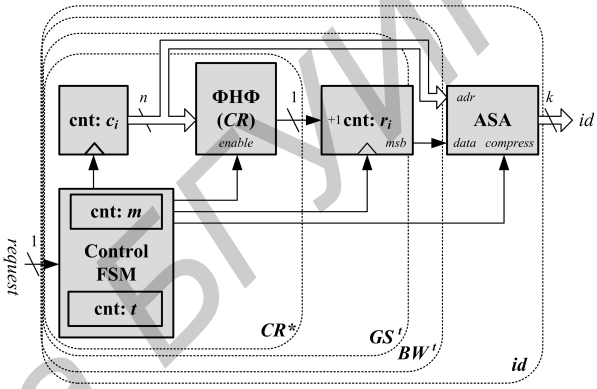

Рис. 2 – Структурная схема аппаратуры идентификации

Структура включает в себя устройство управления (Control FSM), согласующее функционирование остальных блоков, четыре двоичных счетчика(cnt:m, cnt:t, cnt:c_i, cnt:r_i) и адаптивный сигнатурный анализатор (ASA). На рисунке отмечены блоки, отвечающие за последовательное преобразование рассмотренных множеств с целью получения k-разрядного идентификатора id.

Аппаратурные затраты на реализацию предложенной схемы иденификации составляют менее 2% от программируемых ресурсов FPGA Xilinx SPARTAN-3E XCS500E. Верификация предложенной схемы производилась на двух идентичных платах Nexys-2 для которых были получены следующие значения 8-разрядных идентификаторов: $id_1 = 01111000$ и $id_1 = 11101100$.

III. Список литературы

1. Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kenevaar. – London: Springer, 2007. – 344 p.
2. A technique to build a secret key in integrated circuits for identification and authentication application / J.W. Lee [et al.] // VLSI Circuits: Proc. of Symp., Honolulu, Hawai, 17—19 Jun. 2004. — P. 176 — 159.
3. Иванюк, А.А. Проектирование контролепригодных цифровых устройств / А.А. Иванюк, В.Н. Ярмолик. — Минск: Бестпринт, 2006. — 296 с.
4. Digilent Nexys2 Board Reference Manual [Electronic resource]. — Digilent Inc., 2008. — Mode of access: http://digilentinc.com/Data/Products/NEXYS2/Nexys2_rm.pdf. — Date of access: 01.10.2013.