ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ТИПА АРБИТР С МОДИФИЦИРОВАННЫМИ ПУТЯМИ

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

В работе предлагается новый подход для построения схем физически неклонируемой функции типа арбитр с модифицированными путями, обладающими нелинейной конфигурацией. Такой подход позволяет усложнить взаимосвязь запросов и ответов, что потенциально затрудняет построение модели функции с целью осуществления атаки на нее. Приводятся схемотехнические решения предложенных модификаций путей и анализ свойств ФНФ типа арбитр на их основе.

Введение

Физически неклонируемые функции (ФНФ) находят широкое применение в таких областях криптографии как, защита авторских прав на цифровые устройства, неклонируемая идентификация и аутентификация цифровых устройств, генерирование секретных ключей [1] и т.д. По сути ФНФ представляет собой цифровую схему, имеющую множество входов, на которые подаются сигналы запросов, и, как правило, единственный выход, на котором формируется сигнал ответов. Множество пар «запрос-ответ» является уникальным для каждой физической реализации ФНФ, и может быть интерпретировано как физический «отпечаток пальца», который является случайным и неконтролируемым со стороны проектировщиков и производителей цифровых устройств.

Среди всего многообразия видов ФНФ выделяют ФНФ типа арбитр (АФНФ) [1], основанную на сравнении двух сигналов, распространяемых по цифровой схеме с конфигурируемыми парами симметричных путей. Классическая схема АФНФ состоит из трех основных блов: генератора тестовых импульсов (ГТИ), блока конфигурируемых путей (БКП), и, собственно, арбитра (АРБ). Блок ГТИ вырабатывает две копии тестового сигнала, которые поступают на входы БКП. В свою очередь конфигурируемые симметричные пути строятся из базовых цифровых элементов перестановочной сети (permutation network) [2], имеющих два информационных входа a и b, управляющий вход ch, и два выхода x и y. При условии $ch = 0$ элемент осуществляет прямую коммутацию сигналов: $x = a$, $y = b$. В противном случае, при $ch = 1$, перекрестную коммутацию: $x = b$, $y = a$. Схема БКП формируется путем линейного последовательного подключения N базовых элементов перестановочной сети с независимым управлением коммутацией каждого из них сигналами ch_i ($i \in [0; N-1]$), объединенными в единую N-разрядную шину запроса CH.

Таким образом, БКП формирует 2^N различных пар путей. Две копии тестового сигнала поступают на входы первого элемента a_0 и b_0, а два выхода последнего элемента x_{N-1} и y_{N-1} поступают на соответствующие входы арбитра, который осуществляет сравнение двух сигналов и по результату сравнения вырабатывает бит ответа $R \in \{0, 1\}$. При реализации классической схемы АФНФ часто используют следующие ограничения: ГТИ вырабатывает две копии фронта цифрового импульса, в качества схемы АРБ применяют синхронный D-триггер, на вход данных и синхронизации которого поступают сигналы с выходов x_{N-1} и y_{N-1}. Подобная конфигурация обладает рядом недостатков, среди которых можно выделить линейную структуру схемы БКП, которая влечет за собой наличие уязвимости к атакам со стороны злоумышленников с целью обладания точной математической моделью конкретного экземпляра АФНФ. Для усложнения проведения таких атак, в том числе с применением методов машинного обучения, применяются различные защитные алгоритмы и схемы. В данной работе рассматривается альтернативный подход, основанный на построении нелинейных структур БКП, что потенциально усложняет понимание природы формирования пар (CH_j, R_j) $(\forall j \in [0, 2^N - 1])$ для АФНФ.

I. Синтез модифицированных путей

Введем обозначение i-го элемента БКП через α_i. Тогда структуру БКП классической схемы АФНФ можно формально представить следующей записью: $BCP : (\alpha_0, \alpha_1, \alpha_2, ..., \alpha_{N-1}) = \{\alpha\}^N$. Введем три дополнительных элемента: β — демультиплексор $2 \times k$ (с двумя входами и k выходами); γ — элемент перестановочной сети $k \times k$ и δ — мультиплексор $k \times 2$. Элемент β представляет собой специализированную схему, которая обеспечивает прямую и перекрестную коммутацию двух входных сигналов на произвольную пару выходных сигналов из C_k^2 возможных. Элемент γ осуществляет все возможные $k!$ перестановок входных сигналов с их трансляцией на k выходов. Третий элемент δ обеспечивает выборку всех возможных пар входных сигналов и их прямую и перекрестную коммутацию с двумя выходами. Выбирая различные значения k

и реализовывая различные комбинации элементов α, β, γ и δ открываются широкие возможности для построения нелинейных структур БКП, позволяющих различными способами конфигурировать пары путей. Ниже приведены примеры некоторых из возможных вариантов модификаций БКП:

1. $\{\alpha\}^l\beta\delta$;
2. $\{\alpha\}^l\beta\delta\{\alpha\}^m$;
3. $\{\alpha\}^l\beta\{\gamma\}^m\delta\{\alpha\}^p$;
4. $\{\alpha\beta\gamma\delta\}^l$.

Рассмотрим варианты реализаций приведенных элементов для случая $k = 4$. Так, элемент β может быть синтезирован на основе двух элементов α, как это показано на рис. 1.

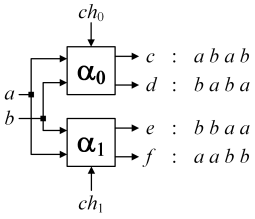

Рис. 1 – Схема элемента β для $k = 4$.

Элемент γ может быть построен на основе хорошо известной схемы [3] с добавлением блока α_5 с фиксированным значением запроса, необходимый для соблюдения структурной симметрии конфигурируемых путей (рис. 2).

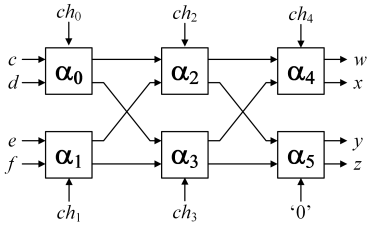

Рис. 2 – Схема элемента γ для $k = 4$.

Схема всевозможных прямых и перекрестных коммутаций двух выходных портов с четырьмя входными представлена на рисунке 3. Представленная на этом же рисунке схема преобразования запросов необходима для выборки пары различных входных сигналов.

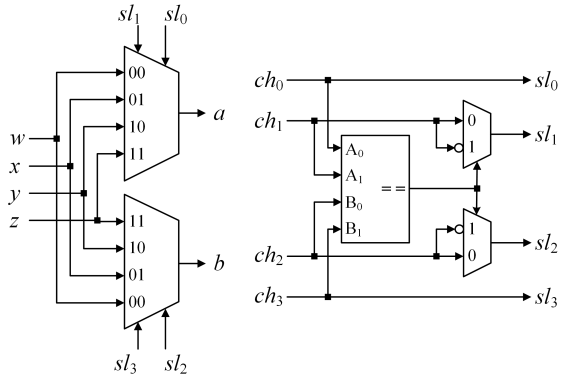

Рис. 3 – Схема элемента δ для $k = 4$ и схема преобразования запросов.

II. Сравнительный анализ

Для проведения анализа предложенного подхода к синтезу элементов БКП была спроектирована экспериментальная установка на основе платы быстрого прототипирования Digilent ZYBO Z7 с FPGA класса ZYNQ. При помощи языка VHDL были созданы проектные описания двух схем с одинаковой разрядность запроса $N = 32$: схема классической АФНФ, для которой БКП описывается конфигурацией $BCP_1 : \{\alpha\}^{32}$, и схема АФНФ с БКП нелинейной конфигурации $BCP_2 : \{\alpha\}^3\beta\{\gamma\}^4\delta\{\alpha\}^3$ для $k = 4$. Реализация БКП классической схемы АФНФ на FPGA занимает 64 блока LUT2, а рассматриваемая схема БКП с нелинейной конфигурацией — 64 LUT2, два блока LUT4, и два блока LUT6. Две схемы оценивались по следующим основным характеристикам ФНФ [4]: стабильность (S) и единообразие (Un).

В таблице приведены средние, максимальные и минимальные значения перечисленных характеристик, полученных на 32 экземплярах обоих конфигураций схем АФНФ.

Таблица 1 – Значения характеристик

S	$avg(S)$	$max(S)$	$min(S)$
BCP_1	0.995323	1.0	0.99319
BCP_2	0.993566	1.0	0.97043
Un	$avg(Un)$	$max(Un)$	$min(Un)$
BCP_1	0.725251	0.8713	0.55254
BCP_2	0.682644	0.92412	0.2018

III. Заключение

В работе предложен новый подход для синтеза блока конфигурируемых путей физически неклонируемой функции типа арбитр. Было предложено использовать три составных элемента, которые позволяют формировать нелинейные модификации путей, что потенциально усложняет сторонние атаки на АФНФ с целью построения ее точной математической модели. Анализ результатов проведенных экспериментов показал состоятельность и перспективность предложенного подхода.

IV. Список литературы

1. A technique to build a secret key in integrated circuits for identification and authentication applications / J.W. Lee [et al.] // Proc. of Intern. Symp. VLSI Circuits (VLSI'04), Honolulu, Hawaii, USA, 7–19 June 2004. — Honolulu, 2004. — P. 176–179.
2. Kannan, R. The KR-Benes Network: A Control-Optimal Rearrangeable Permutation Network / R. Kannan // IEEE Transactions on Computers. —2005. — № 5(54). — P.534-544.
3. Waksman, A. A Permutation Network /A. Waksman // Journal of the ACM. — 1968. — №1(15). — P.159-163.
4. Maiti, A. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions / A. Maiti, V. Gunreddy, P. Schaumont. In: Athanas, P., Pnevmatikatos, D., Sklavos, N. (eds.) Embedded Systems Design with FPGAs. Springer, New York, NY, 2013. — P. 245–267.