УДК 004.056.53

ПРИМЕНЕНИЕ МНОГОПОРТОВОГО S-ПАРАМЕТРИЧЕСКОГО АНАЛИЗА В РЕВЕРС-ИНЖИНИРИНГЕ ИНТЕГРАЛЬНЫХ СХЕМ ДЛЯ ДЕТЕКТИРОВАНИЯ СКРЫТЫХ ФУНКЦИИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ И АНОМАЛИЙ В ПЕРЕДАЧЕ СИГНАЛОВ

А.Б. Батыргалиев, А.А. Молганов
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан

Аннотация. Процесс проектирования интегральных микросхем в нынешнее время сопряжен с определенными технологическими нормами суть которых заключается в уменьшении подаваемой тока, уменьшении расстояния между структурными элементами и увеличения вычислительных мощностей на единицу площади. В связи с этим проведение инженерно-технического анализа на предмет наличия недекларированных возможностей представляется огромной проблемой как с технической точки зрения, так и с юридической – ввиду отсутствия конструкторской документации на интегральную микросхему. Интегральные микросхемы предназначенные для передачи информации с помощью радиочастотных структур имеют особое топологическое строение и поэтому реверс-инжиниринг данных микросхем затруднен из-за наличия фильтров и других помех блокирующих частей. Применение многопортового *S*-параметрического анализа позволяет провести топологический анализ скрытых цепей и портов, определить скрытые режимы работы и паразитных излучений.
Ключевые слова: интегральная микросхема; S-параметр; техническая защита информации; реверс-инжиниринг; печатная плата; инвазивные методы анализа; неинвазивные методы анализа.

APPLICATION OF MULTIPORT S-PARAMETRIC ANALYSIS IN REVERSE ENGINEERING OF INTEGRATED CIRCUITS TO DETECT HIDDEN FUNCTIONAL CAPABILITIES AND ANOMALIES IN SIGNAL TRANSMISSION

A.B. Batyrgaliev, A.A. Molganov
Satbayev Univeristy, Almaty, Republic of Kazakhstan

Abstract. The process of designing integrated circuits at the present time is associated with certain technological standards, the essence of which is to reduce the supplied current, reduce the distance between structural elements and increase computing power per unit area. In this regard, conducting an engineering and technical analysis for undeclared capabilities is a huge problem both from a technical point of view and from a legal one, due to the lack of design documentation for an integrated circuit. Integrated circuits designed to transmit information using radio frequency structures have a special topological structure, and therefore reverse engineering of these chips is difficult due to the presence of filters and other interference from blocking parts. The use of multiport *S*-parametric analysis allows for topological analysis of hidden circuits and ports, to determine hidden modes of operation and spurious emissions.
Keywords: integrated circuit; S-parameter; technical information protection; reverse engineering; printed circuit board; invasive methods of analysis; non-invasive methods of analysis.

Введение

Высокоскоростные радиочастотные интегральные схемы имеют внутреннее топологическое строение в виде много сегментных уровней с абсолютной уровнем металлизации и проявления в процессе производства, в следствие чего становится затруднительно с технической точки зрения провести комплексный и системный анализ на предмет наличия недекларированных возможностей интегральных микросхем с высокой степенью плотности. Анализ с помощью S-параметров позволяет исследовать характеристики передаваемого сигнала между интегральными микросхемами, расположенными на печатной плате, а также выявить паразитные связи между внутренними элементами и дать комплексную оценку влияния различных элементов на преднамеренное или умышленное искажение данных. Изучение

коэффициентов отражения и передачи сигнала помогает на этапе технической экспертизы или сертификации устройства, позволяет оценить потенциальные аппаратные закладки и недекларированные интерфейсы внутри интегральной микросхемы.

Основная часть

Современные системы на кристалле (SoC), в основе своей представляют несколько интегральных микросхем, объединенных высокоскоростным соединением с высокой степенью топологии, и включает в себя сложные многослойные структуры, состоящие из передатчиков, мостов, сетей и приемников. Для оценки характеристик передачи сигнала в таких системах широко применяется анализ S-параметров, который позволяет исследовать коэффициенты отражения и передачи на различных участках сигнальной передачи [1].

В эпоху глобализации и роста экспортного производства аппаратного обеспечения критической информационной инфраструктуры, вопросы информационной безопасности и аппаратного контроля за такими системами, становятся все более актуальными в связи с множественными случаями внедрения аппаратных закладок на этапе производства и упаковки интегральных микросхем. Таким образом, производители интегральных микросхем могут намеренно или якобы случайно оставлять дополнительные функциональные возможности, которые не задокументированы и нереализованны в технической документации или системном программном обеспечении, но могут влиять на работу системы с точки зрения информационной безопасности. Одним из подходов к выявлению таких возможностей является исследование характеристик рассеяния сигнала с помощью S-параметрического анализа. Этот метод позволяет обнаружить паразитные связи, неявные пути передачи данных и изменения в отклике системы, которые могут свидетельствовать о наличии аппаратных закладок или скрытых каналов связи внутри интегральной микросхемы или определенного участка топологии печатной платы.

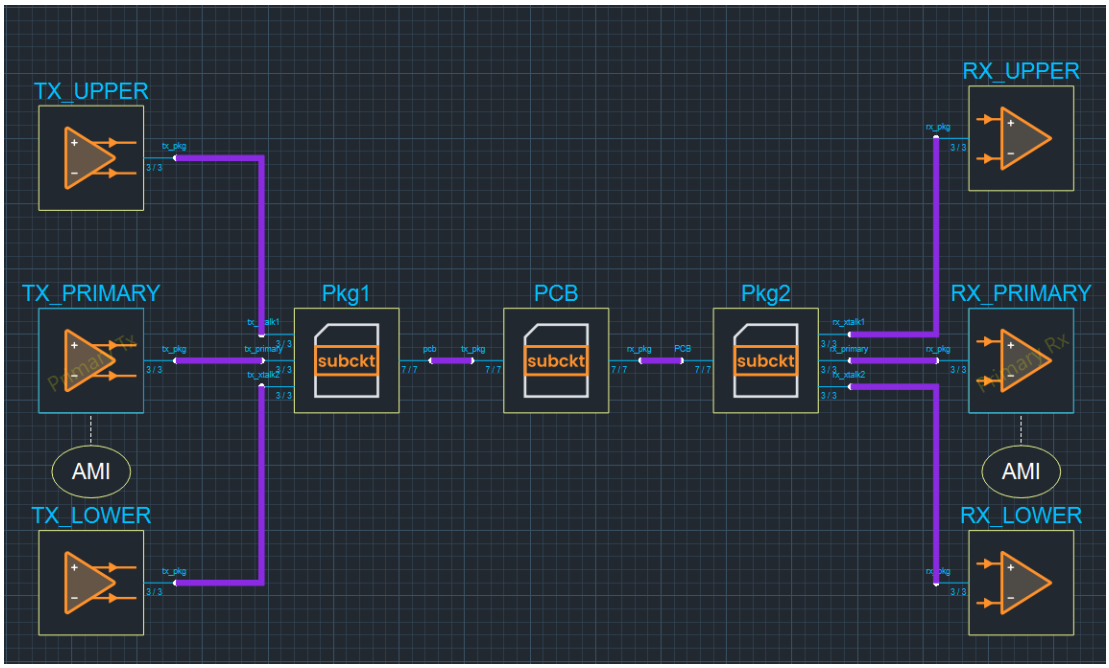

Рис. 1. Пример симуляционного стенда для анализа воздействия скрытых каналов связи
Fig. 1. Example of a simulation stand for analyzing the effects of hidden communication channels

На примере симуляционного виртуального стенда, выполненного в системе автоматизированного анализа Cadence Topology Workbench 2024.010, будет продемонстрировано применение многопортового S-параметрического анализа для выявления недекларированных возможностей на участке топологии печатной платы с двумя интегральными микросхемами [4].

На представленном выше изображении показана структурная схема передачи высокоскоростного сигнала через систему, состоящую из множества последовательно соединенных элементов между собой. Передающие устройства интегральной микросхемы №1 – TX_UPPER, TX_PRIMARY, TX_LOWER, генерируют сигнал, который проходит через соединительный слой интегральной микросхемы (Pkg1), затем передается на дорожку которая располагается на топологии печатной платы (PCB) и затем поступает в соединительный слой интегральной микросхемы №2 (Pkg2), после чего достигает приемных узлов – RX_UPPER, RX_PRIMARY и RX_LOWER.

Для обеспечения корректности симуляции и получения достоверных данных, передача сигнала в процессе симуляции, применяется AMI-модели (Algorithmic Modeling Interface), которые выполняют адаптивную обработку сигнала и компенсируют возникающие искажения путем фильтрации и различных преобразований сигнала. При этом на каждом этапе передачи, сигнал может подвергаться различным воздействиям, таким как потери, перекрестные наводки, отражения и паразитные резонансы. Вследствие этих факторов возможны изменения в характеристиках передачи, которые могут быть выявлены с помощью анализа *S*-параметров.

Signal Name	Data Rate (Gbps)	Baud Rate (GBaudPS)	Stimulus Pattern	Stimulus Offset (ns)	Leading Bits	Tx IO Model	Tx Jitter & Noise	Status
*	*	*	*	*	*	*	*	*
▼ ☑ Signal	5	5	PRBS(seed: 1, poly: 7)	0				
☑ pos	5	5	PRBS(seed: 1, poly: 7)	0		nmos_diff_tx		Signal
☑ neg	5	5	PRBS(seed: 1, poly: 7)	0		nmos_diff_tx		Signal

Рис. 2. Характеристики симулируемого сигнала
Fig. 2. Characteristics of the simulated signal

Для корректной симуляции, необходимо также задать физические величины и другие данные со следующими характеристиками:

1. *Передаваемый сигнал*:

– используется дифференциальный сигнал, состоящий из двух компонентов: положительного (pos) и отрицательного (neg);

– передача осуществляется со скоростью 5 Гбит/с (битрейт) и аналогичной символьной скоростью 5 Гбод/с (NRZ-кодирование).

2. *Структура передаваемых данных*:

– для моделирования используется псевдослучайная битовая последовательность (PRBS) с полиномом 7-го порядка (poly: 7, seed: 1). PRBS применяется для имитации реального трафика и оценки качества передачи сигнала;

– смещение сигнала во времени отсутствует (Stimulus Offset = 0 нс), что означает, что передача начинается без задержек.

3. *Модель передатчика*:

– передатчик использует NMOS-дифференциальный драйвер (Tx IO Model = nmos_diff_tx), что стандартизировано ввиду использования идентичной модели драйвера в современных высокоскоростных интерфейсах – PCIe, USB, SerDes.

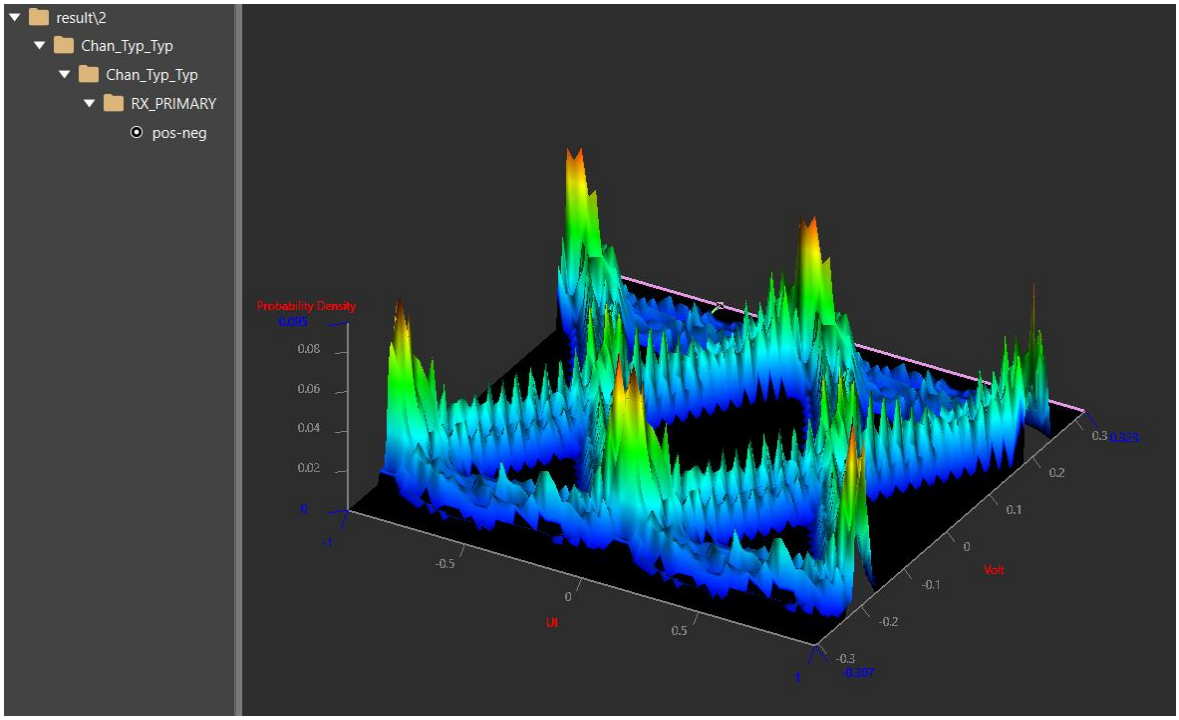

Рис. 3. Характеристики симулируемого сигнала
Fig. 3. Characteristics of the simulated signal

На представленном изображении показана трехмерная визуализация вероятностного распределения дифференциального сигнала, полученного в процессе моделирования высокоскоростного канала передачи данных. График демонстрирует зависимость плотности вероятности (Probability Density) от напряжения (Volt) и временного интервала (UI – Unit Interval), что позволяет оценить качество передаваемого сигнала от одной интегральной микросхемы к другой [5].

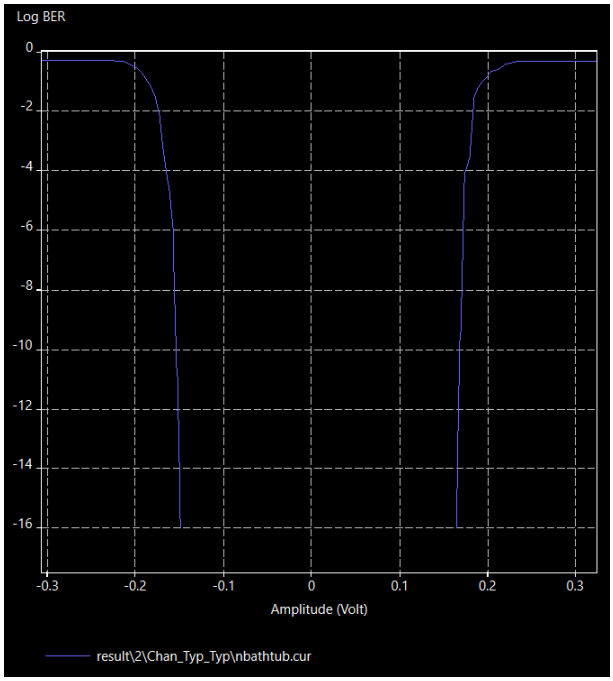

Рис. 4. График сигнала с помехами в приемнике интегральной микросхемы №2
Fig. 4. Graph of the signal with interference in the receiver of integrated circuit No. 2

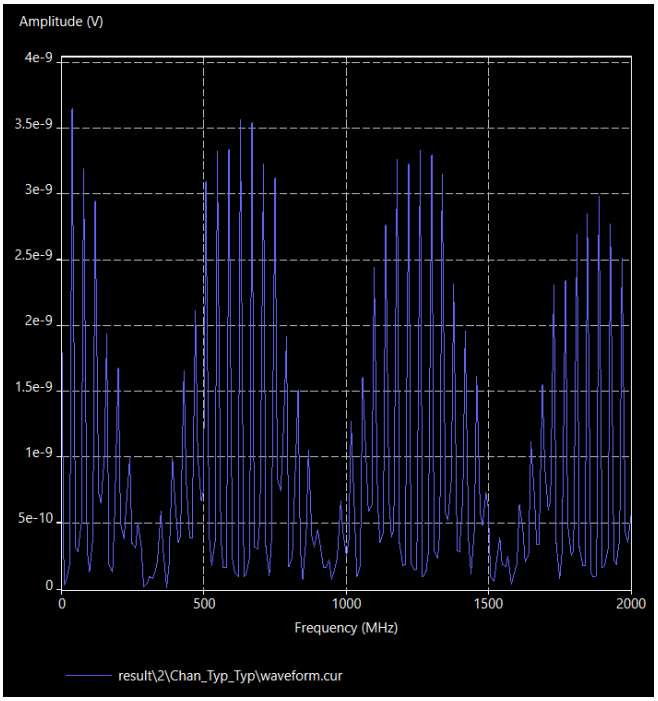

Рис. 5. График сигнала с помехами в приемнике интегральной микросхемы №2
Fig. 5. Graph of the signal with interference in the receiver of integrated circuit No. 2

Представленные графики с результатами симуляции, свидетельствует о наличии двух областей с высокой вероятностью ошибок (на краях амплитудного диапазона) и центральной зоны с минимальным уровнем BER-значения. Это типично для систем с разделением сигналов на дискретные уровни, таких как двоичные или многоуровневые модуляции (NRZ или PAM-4 модуляция). Минимизация ошибок в центральной зоне подтверждает эффективность используемых схем синхронизации, эквализации и кодирования коррекции ошибок. В то же время, резкие границы областей ошибок могут указывать на чувствительность системы к внешним помехам, фазовому шуму или дрожанию сигнала зависящих от внешнего источника генерации электромагнитных излучений [3].

Полученные результаты позволяют сделать несколько выводов. Во-первых, центральная область графика является ключевой для надежной передачи данных, и любые изменения параметров системы должны стремиться к расширению этой зоны. Во-вторых, высокая плотность ошибок на краях амплитудного диапазона указывает на необходимость оптимизации схем передачи и приема, в частности, улучшения тактового восстановления и фильтрации сигнала с помощью блоков ADC/DAC и умножителей/делителей. В-третьих, анализ формы кривой может помочь в калибровке параметров передатчика и приемника для достижения оптимального соотношения между мощностью сигнала и вероятностью ошибки [2].

Дополнительно, выявленные аномалии в распределении сигнальных ошибок, неожиданные искажения сигнала или нехарактерное поведение системы при определенных режимах работы могут указывать на наличие скрытых аппаратных закладок. Поэтому анализ кривых BER-значений позволяет выявить потенциальные отклонения, которые могут свидетельствовать о попытках несанкционированного вмешательства в работу интегральной микросхемы или системы на кристалле.

В заключении, можно сделать вывод что исследование представленных характеристик сигнала подтверждает важность использования логарифмического анализа BER-значений для проектирования, отладки и исследования цифровых систем

передачи данных. Данный вид анализа позволяет выявлять потенциальные проблемы на этапе исследования интегральной микросхемы на предмет наличия недекларированных возможностей.

Список использованных источников

1. Al-Meer, A., & Al-Kuwari, S. (2023). Physical Unclonable Functions (PUF) for IoT Devices. ACM Computing Surveys.
2. Liang, W., Xie, S., Zhang, D., Li, X., & Li, K.-C. (2022). A Mutual Security Authentication Method for RFID-PUF Circuit Based on Deep Learning. ACM Transactions on Internet Technology.
3. Nagata, M., Miki, T., & Niura, N. (2022). Physical Attack Protection Techniques for IC Chip Level Hardware Security. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems.
4. Hemavathy, S., & Bhaaskaran, V. S. K. (2023). Arbiter PUF - A Review of Design, Composition, and Security Aspects. IEEE Access.
5. Khichel, D., & Moradi, A. (2022). Low-Latency Hardware Private Circuits. Proceedings of the ACM Conference on Computer and Communications Security

References

1. Al-Meer, A., & Al-Kuwari, S. (2023). Physical Unclonable Functions (PUF) for IoT Devices. ACM Computing Surveys.
2. Liang, W., Xie, S., Zhang, D., Li, X., & Li, K.-C. (2022). A Mutual Security Authentication Method for RFID-PUF Circuit Based on Deep Learning. ACM Transactions on Internet Technology.
3. Nagata, M., Miki, T., & Niura, N. (2022). Physical Attack Protection Techniques for IC Chip Level Hardware Security. IEEE Transactions on Very Large-Scale Integration (VLSI) Systems.
4. Hemavathy, S., & Bhaaskaran, V. S. K. (2023). Arbiter PUF - A Review of Design, Composition, and Security Aspects. IEEE Access.
5. Khichel, D., & Moradi, A. (2022). Low-Latency Hardware Private Circuits. Proceedings of the ACM Conference on Computer and Communications Security

Сведения об авторах

Батыргалиев А.Б., Доктор Ph.D., ассоциированный процессор, Кафедра Кибербезопасности, обработки и хранения информации, Институт автоматики и информационных технологий, Казахский национальный исследовательский технический университет имени К. И. Сатпаева, a.batyrgaliev@su.edu.kz
Молганов А.А., магистрант ОП «Комплексное обеспечение информационной безопасности», Кафедра Кибербезопасности, обработки и хранения информации, Институт автоматики и информационных технологий, Казахский национальный исследовательский технический университет имени К. И. Сатпаева, a.molganov@su.edu.kz

Information about the authors

Batyrgaliev A.B., Ph.D., Associate Professor, Department of Cybersecurity, Information Processing and Storage, Institute of Automation and Information Technology, Satbayev University, a.batyrgaliev@su.edu.kz.
Molganov A.A., Master's student in the Department of Integrated Information Security, Department of Cybersecurity, Information Processing and Storage, Institute of Automation and Information Technology, Satbayev University, a.molganov@su.edu.kz.