УДК 621.368

К. К. Кондрашов, М. И. Ершов, А. О. Гасников
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Современное состояние диагностики микропроцессорных систем по нетрадиционным побочным каналам

Рассмотрены основные принципы и методы диагностики микропроцессорных систем по нетрадиционным побочным каналам. Особое внимание уделено анализу микроконтроллеров по энергопотреблению. На основании анализа литературных источников представлено современное состояние разработок в области информационной безопасности микропроцессорных систем.

Диагностика микропроцессорных систем, побочные каналы, энергопотребление микросхем, информационная безопасность

Микропроцессорные системы являются неотъемлемой частью электроники и входят в состав схем практически любой техники всевозможного назначения. В условиях непрерывного развития электронных устройств, а также постоянного увеличения их количества во всех областях жизни и деятельности человека важную роль приобретает диагностика их компонентов на соответствие предъявляемым требованиям. Так как микропроцессорные системы отвечают за обработку и хранение информации, в том числе конфиденциальной, применение в технике современной компонентной базы влечет за собой необходимость принятия мер по обеспечению информационной безопасности. Данная проблема получила широкое распространение в течение последних двух десятилетий, что в первую очередь обусловлено появлением и интенсивным развитием методов организации несанкционированного доступа к микропроцессорным системам, имеющим классическую защиту. В настоящее время одним из наиболее популярных направлений стал анализ интегральных микросхем по нетрадиционным побочным каналам (Side Channel Analysis – SCA), который обладает большими возможностями и представляет собой мощный инструмент неразрушающей диагностики электронной компонентной базы.

В рамках представленного обзора приводится описание известных методов анализа микропроцессорных систем по побочным каналам и способов предотвращения доступа к информации.

Анализ по побочным каналам можно определить как совокупность методов и технологий получения данных из экспериментально измеряемых характеристик работающей интегральной микросхемы. К ним относятся времена выполнения операций, энергопотребление, электромагнитное излучение, температура корпуса и тепловое излучение, акустические шумы и механические колебания. Активные разработки данного направления начались с выявления уязвимости криптосистем в электронных смарт-картах [1], [2]. Многочисленные исследования показали возможность вскрытия шифра, хранящегося в памяти, с помощью атаки по побочным каналам [3], [4]. Вскоре было установлено, что наиболее распространенные системы шифрования и большинство применяемых чипов не имеют никакой защиты от подобных атак. Вместе с тем, в результате многолетних исследований были выработаны основные способы получения и анализа сигналов, обычно детектируемых на побочных каналах устройств.

Традиционным методом неразрушающей диагностики микросхем является доступ по потребляемой мощности [5], [6]. Физические основы метода состоят в том, что при переключении логических элементов возникают импульсы тока, величина которых на практике определяется динамической нагрузкой схемы. В общем случае на амплитуды импульсов могут влиять многие факторы, среди которых выделяют внешние и внутренние. К внешним факторам относятся различные шумы, возникающие вследствие влияния температуры, наводок от электромагнитных полей, воздействия измерительного оборудования и др. Эти шумы, как правило, удается устранить при первичной обработке сигнала с применением программных фильтров. Внутренние факторы представляют собой флуктуации потребляемой мощности вследствие процессов, происходящих в устройстве. Появляющиеся колебания могут быть вызваны различными источниками, но они имеют общую природу и обусловлены конструктивно-схемотехническими особенностями исследуемого устройства. Для реализации доступа по шине питания в качестве базового предположения выступает некоторая зависимость амплитуды и частоты следования импульсов тока от процессов, происходящих в микросхеме [7], [8]. Частота наблюдаемых импульсов непосредственно связана с частотой тактового генератора микропроцессорной системы, в большинстве случаев они полностью совпадают. Амплитуда скачков тока при выполнении системных операций зависит в первую очередь от того, какие именно логические элементы и в каком количестве переключаются на текущем такте работы [9]. Состояние схемы в фиксированный момент времени образует ее динамическую нагрузку, в упрощенном представлении величина этой нагрузки однозначно характеризует энергопотребление устройства. Несмотря на то что современные микросхемы могут находиться во множестве различных состояний с почти одинаковыми значениями потребляемого тока, наличие даже слабо выраженной и едва проявляющейся зависимости позволяет произвести анализ исполняемой программы и установить хранящуюся в памяти информацию [4].

Приборная реализация доступа по потребляемой мощности относительно проста [6]. В общем случае для проведения измерений требуется осциллограф с достаточно высоким разрешением по входному сигналу. Также может понадобиться резистор небольшого номинала, включаемый последовательно в цепь питания исследуемого устройства. Напряжение может сниматься как с

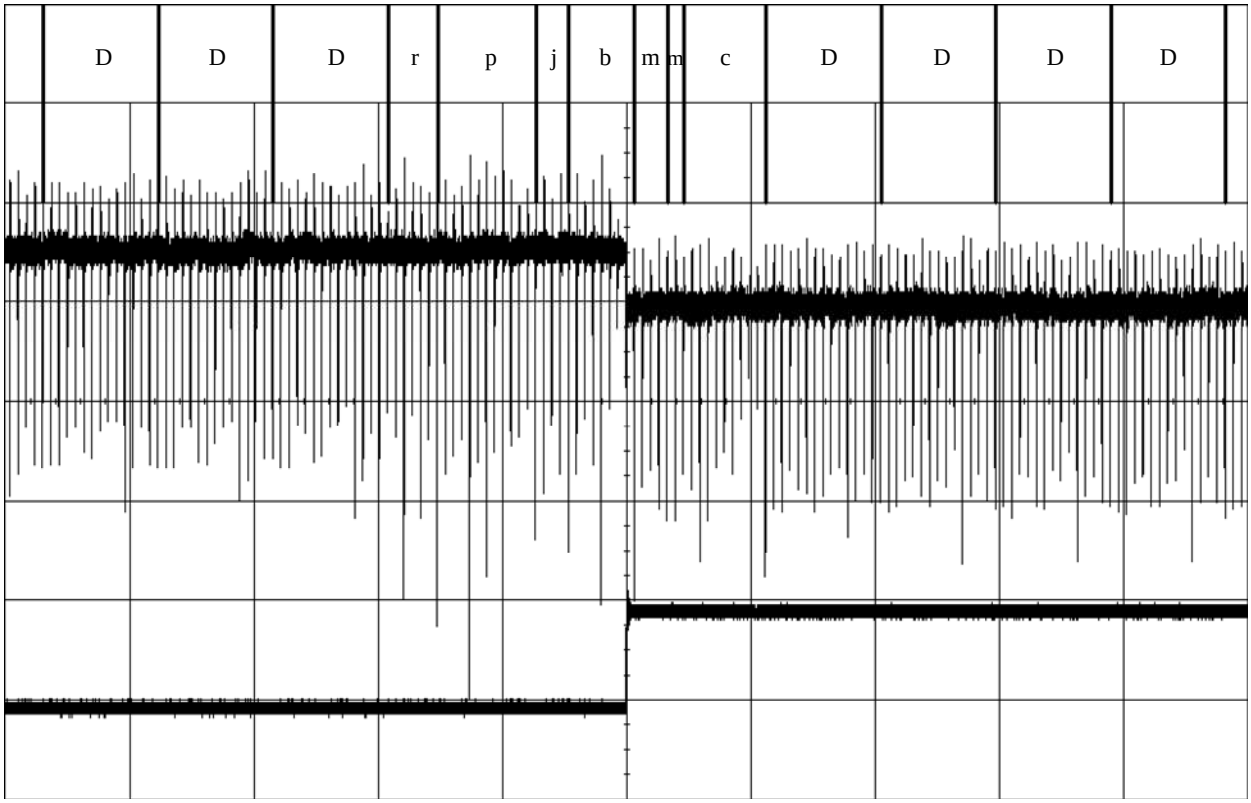

Рис. 1

резистора, так и с разъема питания самой микросхемы. Второй вариант традиционно используется при анализе микроэлектронных компонентов на платах приборов, когда наличие обвязки необходимо для их нормального функционирования в соответствии с заложенной программой. При исследованиях слабых и шумящих сигналов возможно применение в цепи измерений предварительных усилителей, фильтров и т. п.

Существуют различные способы анализа полученного сигнала [4]–[6], [8], [10]. Обычно их разделяют на три вида по возрастанию сложности [3]:

1) простой анализ питания (ПАП);

2) дифференциальный анализ питания (ДАП);

3) дифференциальный анализ питания высокого порядка (ДАП-ВП).

На практике, в зависимости от поставленной задачи, обработка сигнала осуществляется последовательно все более сложными способами по мере надобности. Выявляемая на каждом новом уровне информация часто помогает конкретизировать задачу и сформулировать условия для ее решения другими методами. Если особенности сигнала на шине питания микросхемы изучены достаточно хорошо, ее анализ проводится в сокращенном формате на основе уже имеющихся данных, благодаря чему уменьшаются затраты времени.

Простой анализ питания подразумевает прямую интерпретацию детектируемых колебаний потребляемого тока. В рамках данного подхода предполагается, что амплитуды и частоты следования импульсов на осциллограмме дают некоторую информацию о процессах, происходящих в устройстве [3], [5], [6], [8]. Так, например, во многих микроконтроллерах отдельные модули тактируются от собственных генераторов на частотах, отличающихся от частоты центрального ядра. Поэтому наблюдаемое изменение интервала времени между импульсами может свидетельствовать о работе того или иного модуля. Распределение амплитуд импульсов на выбранном участке сигнала, как правило, имеет характерные признаки, по которым их можно объединить в группы, соответствующие выполняемым операциям. Исходной точкой для разбивки сигнала может быть операция записи бита в порт ввода-вывода (рис. 1, обозначения команд: D – Delay; r – ret; p – cmp; j – jnz; b – bis; m – mov; c – call). Таким образом, подобные действия уже позволяют получить ценные сведения о программном коде, а также они подготавливают фундамент для последующих этапов анализа.

Дифференциальный анализ питания заключается в использовании статистических методов обработки данных эксперимента [3], [5], [7], [8]. Этот способ исследований основан на сопоставлении нескольких сигналов, снятых с шины питания при различных вариантах исполнения одних и тех же инструкций. Предварительная стадия включает в себя сохранение большого числа детектируемых сигналов, синхронизацию их однотипных участков по времени и арифметическое усреднение амплитуд импульсов, соответствующих операциям с одинаковыми числами. На следующей стадии при помощи визуального анализа или математического аппарата осуществляется поиск возможной корреляции между средними значениями амплитуд и числами, которые каким-либо образом обрабатываются устройством в текущем такте (например, четыре операции сравнения разных чисел отчетливо видны на рис. 2, однако их амплитуды не полностью совпадают). Если эти числа считываются из флэш-памяти микросхемы, обнаруженная зависимость является ключом к восстановлению ее содержимого.

Дифференциальный анализ питания высокого порядка отличается тем, что амплитуда импульсов предполагается зависимой от нескольких факторов одновременно, причем среди них могут быть как числа, так и пути прохождения сигналов, состояния служебных регистров и т. п. [3], [11]–[13]. В таком варианте поиск корреляции требует построения более сложных моделей, которые учитывают совместное влияние многих величин. На практике обычно применяются эмпирические модели, их разработка менее трудоемка и достаточно быстра. Формально они выражены в виде таблиц или формул, устанавливающих зависимость амплитуды от воздействующих факторов в числовом представлении. Порядок анализа определяется количеством независимых величин, входящих в выбранную модель.

При создании устройств, связанных с обработкой конфиденциальной информации, часто возникает необходимость в защите микросхем от несанкционированного доступа по побочным каналам. Различают три метода противодействия атакам по энергопотреблению [3]–[8]:

Рис. 2

1) модификация кода программы;

2) конструкторско-схемотехническая модификация кристалла;

3) модификация логической системы.

Первый способ наиболее прост в реализации и преследует две возможные цели – изменение положения искомого участка сигнала во времени или скрытие критически важных данных посредством дополнительных операций шифрования [14]–[17]. В первом случае перед уязвимыми командами программы вводятся искусственные задержки произвольной длительности. Для большинства микроконтроллеров это делается либо с помощью встроенного таймера со случайным числом циклов, либо путем внесения в программный код набора «пустых» операций. Подобные меры в некоторой степени затрудняют проведение исследований методом ПАП, но не способны эффективно противостоять доступу с использованием ДАП [14]. Во втором случае в исполняемый код добавляются процедуры, обеспечивающие промежуточное шифрование данных перед актами считывания или записи. Для повышения надежности генерация маскирующего байта или целого ключа происходит автоматически при каждом обращении к памяти микросхемы [15], [16]. Такая защита значительно осложняет анализ сигнала, детектируемого на любом побочном канале.

Второй способ подразумевает применение в составе устройства одного или нескольких элементов, препятствующих выделению информации из сигнала на шине питания [5], [8]. Фактически это может быть как схема фильтрации для сглаживания пульсаций потребляемого тока, так и встроенный источник шума, подавляющего анализируемые колебания. Оба варианта хорошо работают против метода ПАП, но не позволяют гарантированно предотвратить доступ в других, более мощных вариантах. Тем не менее, исследование микросхем с подобной защитой часто становится нецелесообразным ввиду резкого роста затрат.

Третий способ является самым эффективным средством противодействия любому из видов доступа по энергопотреблению. Его ключевая идея состоит в использовании сложных динамических логических систем [18]–[20]. Поскольку все виды анализа полученного сигнала основаны на наличии зависимости между эквивалентной нагрузкой схемы и текущими информационными процессами, операции с периодически изменяющимися логическими уровнями и неопределенной величиной потребления не могут быть идентифицированы в рамках традиционных методов. Не-

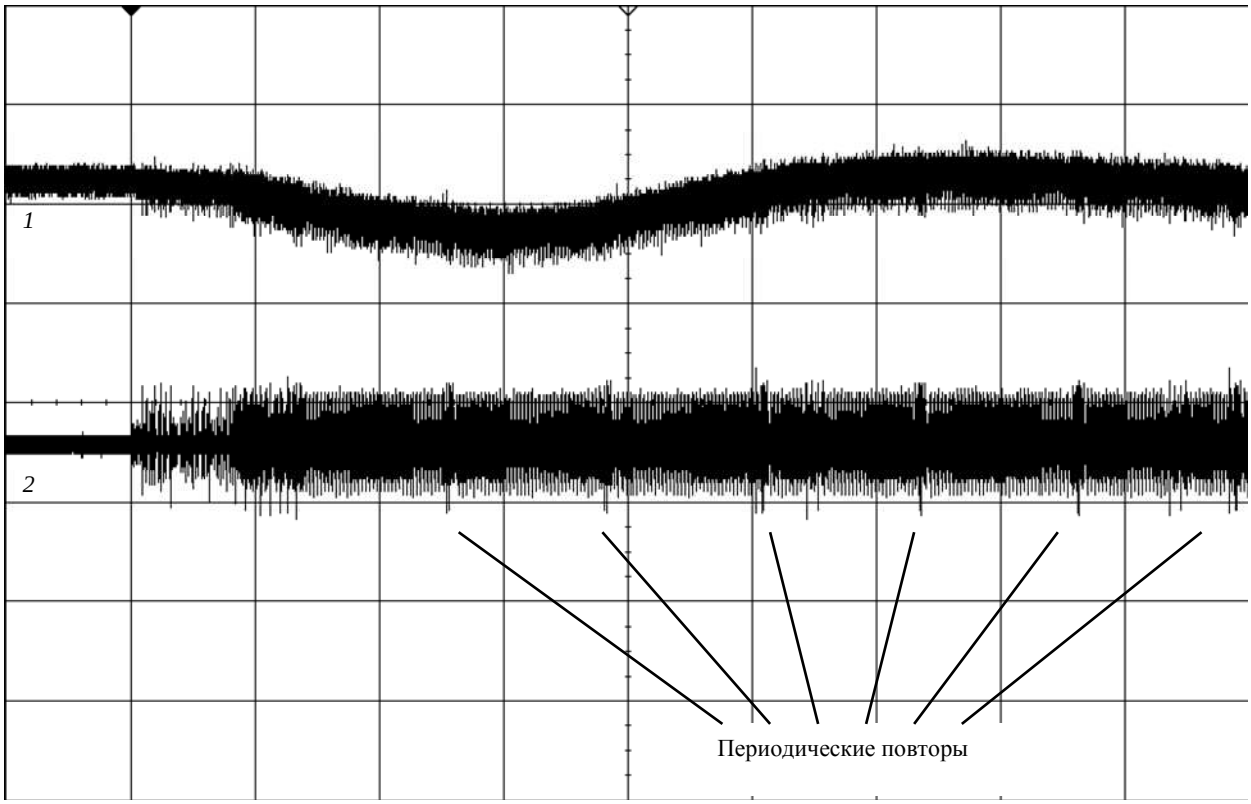

Рис. 3

смотря на высокую степень защищенности устройств с указанной системой, их разработка достаточно трудоемка и, как следствие, не всегда оправдана с экономической точки зрения.

В настоящее время интенсивно развиваются новые методы анализа интегральных микросхем по побочным каналам. Недавно появились исследования, посвященные принципиально новым способам обработки сигналов в ходе классического доступа по энергопотреблению [10], [21]. Авторы этих публикаций рассматривают процедуру перевода полученного сигнала в частотную область с помощью преобразования Фурье или Wavelet-функций. Из построенной диаграммы можно быстро извлечь множество ценных сведений об исполняемом коде, также по ней можно установить значение одного байта, хранящегося во флэш-памяти. Данный подход часто позволяет обойти распространенные типы защиты от доступа по побочным каналам, демонстрируя при этом довольно высокую точность результатов. Некоторые работы сконцентрированы на принципах диагностики микросхем по электромагнитному излучению, которая оказывается исключительно эффективной в ряде случаев [22]–[26]. Сигнал, снимаемый с детектора ближнего поля, имеет характерные особенности, составляющие дополнительный источник информации о процессах в устройстве [27]. К тому же этот вариант анализа полезен при наличии встроенной схемотехнической защиты на шине питания (на рис. 3 показаны сигналы, полученные одновременно на шине питания (*1*) и на детекторе ближнего магнитного поля (*2*) исследуемого устройства). Для противодействия доступу такого рода в конструкцию микросхемы добавляются специальные экраны, формируемые в отдельных слоях на стадии изготовления [25]. Возможности диагностики по другим побочным каналам пока еще изучены слабо.

За последние два десятилетия исследователями в области анализа микроэлектронных устройств по побочным каналам был накоплен значительный опыт восстановления скрытых шифров и ключей криптосистем. В то же время в литературе не получила достаточного внимания проблема комплексной диагностики микросхем неразрушающими методами с возможностью считывания всего содержимого внутренней памяти. Данное направление становится особенно актуальным из-за постоянно возрастающих требований к безопасности как с точки зрения надежного хранения информации, так и с точки зрения обеспечения целостности программного кода. Несмотря на общность ключевых подходов, реализация атак на смарт-карты с целью получения кодов шифрования существенно отличается от анализа более сложных систем, который не предполагает заранее известного алгоритма их функционирования. Наиболее критичным в этом случае является отсутствие возможности изменения входных данных на этапе проведения измерений. Следовательно, для сопоставления наблюдаемых групп импульсов с конкретными числами или операциями необходимо знать зависимость потребляемой мощности от состояния схемы. Эта зависимость обычно строится на основе многочисленных экспериментов по исследованию сигнала, снимаемого с шины питания аналогичного устройства, которое выполняет предварительно заложенную программу. Формально результаты выражаются в виде набора шаблонов, соответствующих всем типовым операциям при любых допустимых значениях системных регистров и шин [28], [29]. Использование библиотек шаблонов позволяет автоматизировать циклы обработки сигнала для семейства микросхем одного класса, что одновременно повышает скорость и точность их диагностики. По этой причине создание функциональных программно-аппаратных комплексов для восстановления информации из памяти микропроцессорных систем представляет собой актуальную задачу.

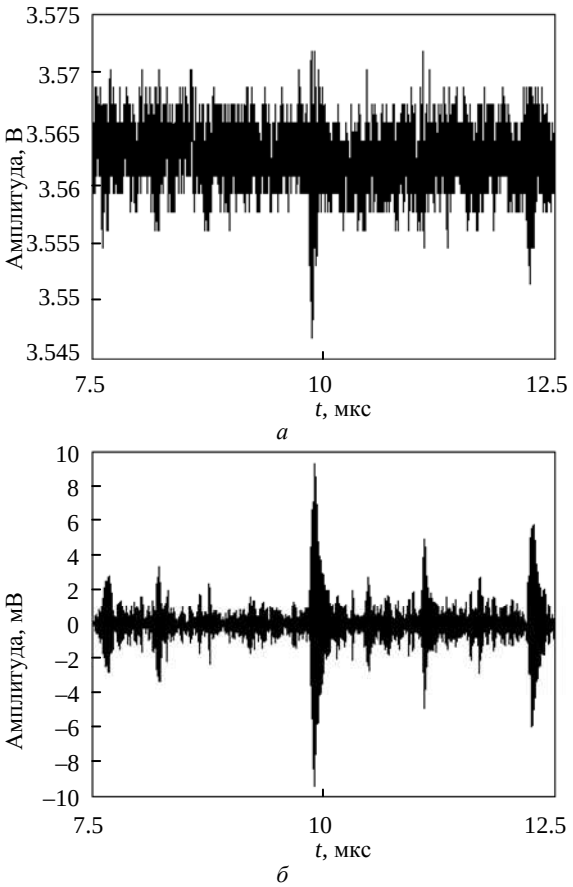

Рис. 4

В настоящее время многочисленные исследования разнообразных микроконтроллеров показывают возможность доступа к внутренним процессам через два уязвимых побочных канала – энергопотребление и электромагнитное излучение (в некоторых случаях). Успехи в области компьютерной обработки сигнала с шины питания уже сейчас позволяют осуществлять фильтрацию шума, поиск содержащих информацию импульсов, вычисление их относительных позиций во времени и сохранение результатов в текстовом или графическом формате (на рис. 4 приведен пример сигнала, снятого с шины питания устройства: *а* – до фильтрации и *б* – после). Вероятнее всего, дальнейшее развитие методов диагностики по побочным каналам будет происходить по двум путям. Один из них заключается в реализации функции автоматизированного распознавания базовых операций по детектируемым колебаниям на основе сформированной библиотеки. Другой состоит в объединении программной и аппаратной части в многофункциональный измерительный комплекс. Оба направления вместе призваны обеспечить высокую гибкость и эффективность диагностики.

СПИСОК ЛИТЕРАТУРЫ

1. Kocher P. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems // Advances in Cryptology – CRYPTO '96. Berlin: Springer-Verlag Berlin Heidelberg, 1996. P. 104–113.

2. A practical implementation of the timing attack / J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems // Smart Card. Research and Applications. Berlin: Springer-Verlag Berlin Heidelberg, 2000. P. 167–182.

3. Проблемы защиты смарт-карт // Украинский ресурс по безопасности. Киев, 1999. URL: http://kiev-security.org.ua/box/19/114 (дата обращения: 10.12.2015).

4. Zhou Y., Feng D. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing // Proc. of NIST Physical Security Testing Workshop, Honolulu, Sept. 26–29, 2005 / Cryptology ePrint Archive. 2005. Report 2005/388. URL: http://ia.cr/2005/388 (дата обращения: 10.12.2015).

5. Kocher P., Jaffe J., Jun B. Differential power analysis // Advances in Cryptology – CRYPTO '99. Berlin: Springer-Verlag Berlin Heidelberg, 1999. P. 388–397.

6. Messerges T., Dabbish E., Sloan R. Examining smart-card security under the threat of power analysis attacks // IEEE Transactions on Computers. 2002. Vol. 51, № 5. P. 541–552.

7. Introduction to differential power analysis / P. Kocher, J. Jaffe, B. Jun, P. Rohatgi // J. of Cryptographic Engineering. 2011. Vol. 1, iss. 1. P. 5–27.

8. Standaert F.-X. Introduction to Side-Channel Attacks // Secure Integrated Circuits and Systems. NY: Springer US, 2010. P. 27–42.

9. Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model // Cryptographic Hardware and Embedded Systems – CHES 2004. Berlin: Springer-Verlag Berlin Heidelberg, 2004. P. 16–29.

10. Tiu C. C. A New Frequency-Based Side Channel Attack for Embedded Systems: Master degree thesis / University of Waterloo. Waterloo, 2005.

11. Messerges T. Using Second-Order Power Analysis to Attack DPA Resistant Software // Cryptographic Hardware and Embedded Systems – CHES 2000. Berlin: Springer-Verlag Berlin Heidelberg, 2000. P. 238–251.

12. Akkar M.-L., Goubin L. A Generic Protection against High-Order Differential Power Analysis // Fast Software Encryption. Berlin: Springer-Verlag Berlin Heidelberg, 2003. P. 192–205.

13. Improved Higher-Order Side-Channel Attacks with FPGA Experiments / E. Peeters, F.-X. Standaert, N. Donckers, J.-J. Quisquater // Cryptographic Hardware and Embedded Systems – CHES 2005. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 309–323.

14. Clavier C., Coron J.-S., Dabbous N. Differential Power Analysis in the Presence of Hardware Countermeasures // Cryptographic Hardware and Embedded Systems – CHES 2000. Berlin: Springer-Verlag Berlin Heidelberg, 2000. P. 252–263.

15. Coron J.-S., Goubin L. On Boolean and Arithmetic Masking against Differential Power Analysis // Cryptographic Hardware and Embedded Systems – CHES 2000. Berlin: Springer-Verlag Berlin Heidelberg, 2000. P. 231–237.

16. Blomer J., Guajardo J., Krummel V. Provably Secure Masking of AES // Selected Areas in Cryptography. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 69–83.

17. Mangard S., Popp T., Gammel B. M. Side-Channel Leakage of Masked CMOS Gates // Topics in Cryptology – CT-RSA 2005. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 351–365.

18. A Design Methodology for Secured ICs Using Dynamic Current Mode Logic / F. Mace, F.-X. Standaert, J. J. Quisquater, J.-D. Legat // Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 550–560.

19. Suzuki D., Saeki M., Ichikawa T. Random Switching Logic: A Countermeasure against DPA based on Transition Probability // Cryptology ePrint Archive. 2004. Report 2004/346. URL: http://ia.cr/2004/346 (дата обращения: 10.12.2015).

20. Razafindraibe A., Robert M., Maurine P. Analysis and Improvement of Dual Rail Logic as a Countermeasure Against DPA // Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation. Berlin: Springer-Verlag Berlin Heidelberg, 2007. P. 340–351.

21. Charvet X., Pelletier H. Improving the DPA attack using Wavelet transform // Proc. of NIST Physical Security Testing Workshop, Honolulu, Sept. 26–29, 2005 / CADSHOP.RU. 2014. URL: http://www.cadshop.ru/articles/4.pdf (дата обращения: 10.12.2015).

22. Gandolfi K., Mourtel C., Olivier F. Electromagnetic Analysis: Concrete Results // Cryptographic Hardware and Embedded Systems – CHES 2001. Berlin: Springer-Verlag Berlin Heidelberg, 2001. P. 251–261.

23. The EM Side-Channel(s) / D. Agrawal, B. Archambeault, J. R. Rao, P. Rohatgi // Cryptographic Hardware and Embedded Systems – CHES 2002. Berlin: Springer-Verlag Berlin Heidelberg, 2003. P. 29–45.

24. Gebotys C. H., Ho S., Tiu C. C. EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA // Cryptographic Hardware and Embedded Systems – CHES 2005. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 250–264.

25. Quisquater J.-J., Samyde D. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards // Smart Card Programming and Security. Berlin: Springer-Verlag Berlin Heidelberg, 2001. P. 200–210.

26. Li H., Markettos A. T., Moore S. Security Evaluation Against Electromagnetic Analysis at Design Time // Cryptographic Hardware and Embedded Systems – CHES 2005. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 280–292.

27. Agrawal D., Rao J. R., Rohatgi P. Multi-channel Attacks // Cryptographic Hardware and Embedded Systems – CHES 2003. Berlin: Springer-Verlag Berlin Heidelberg, 2003. P. 2–16.

28. Chari S., Rao J. R., Rohatgi P. Template Attacks // Cryptographic Hardware and Embedded Systems – CHES 2002. Berlin: Springer-Verlag Berlin Heidelberg, 2003. P. 13–28.

29. Rechberger C., Oswald E. Practical Template Attacks // Information Security Applications. Berlin: Springer-Verlag Berlin Heidelberg, 2005. P. 440–456.

K. K. Kondrashov, M. I. Ershov, A. O. Gasnikov
Saint Petersburg Electrotechnical University «LETI»

SIDE-CHANNEL DIAGNOSTICS FOR MICROPROCESSOR DEVICES: CURRENT STATE

The general approaches and methods of diagnostics for microprocessor devices are described. A lot of attention is taken to the power analysis for microcontroller units. Investigations in the field of information security of microprocessor devices in the current state presented are based on the free articles published in the literature.

Diagnostics for microprocessor devices, side channels, energy consumption of microcircuits, information security