

Метод оценки уязвимости микроконтроллеров к атакам по электромагнитному стороннему каналу

З.К. Фирсов ¹, В.Е. Трифонов ¹, А.Б. Левина ¹

¹Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Россия, 197022, г. Санкт-Петербург

Аннотация. В статье представлен метод оценки уязвимости микроконтроллеров к атакам по электромагнитному побочному каналу. Метод основан на регистрации электромагнитного излучения с помощью программно-определяемого радиоприёмника и корреляционном анализе полученных трасс с использованием модели утечки по весу Хэмминга. Предложенный подход экспериментально исследован на плате Arduino Uno с микроконтроллером ATmega328P, выполняющим шифрование по алгоритму AES-128 с фиксированным секретным ключом. Анализ приблизительно 1000 электромагнитных трасс позволил восстановить все 16 байтов ключа AES-128. Полученные результаты показывают, что корреляционный анализ электромагнитного излучения может применяться для выявления уязвимостей микроконтроллерных реализаций криптографических алгоритмов.

Ключевые слова: атаки по сторонним каналам, электромагнитный анализ, корреляционный анализ мощности, микроконтроллер, AES-128, оценка уязвимости.

Abstract. This article presents a method for assessing the vulnerability of microcontrollers to electromagnetic side-channel attacks. The method is based on recording electromagnetic emissions using a software-defined radio receiver and performing correlation analysis of the acquired traces with a Hamming-weight leakage model. The proposed approach was experimentally evaluated using an Arduino Uno board based on the ATmega328P microcontroller, which performed AES-128 encryption with a fixed secret key. Analysis of approximately 1,000 electromagnetic traces enabled the recovery of all 16 bytes of the AES-128 key. The results demonstrate that correlation analysis of electromagnetic emissions can be used to identify vulnerabilities in microcontroller implementations of cryptographic algorithms.

Keywords: side-channel attacks, electromagnetic analysis, correlation power analysis, microcontroller, AES-128, vulnerability assessment.

Введение

С ростом числа встраиваемых систем и микроконтроллеров, применяемых в критически важных объектах инфраструктуры, обеспечение их защиты от атак по сторонним каналам становится особенно актуальной задачей. Микроконтроллеры широко используются в современных устройствах, от телекоммуникационного оборудования до систем промышленной автоматизации, и именно их компрометация может привести к утечке конфиденциальной информации и нарушению работы всей системы [1, 2].

Микроконтроллер представляет собой специализированную интегральную схему, которая может выполнять криптографические операции, обеспечивать аутентификацию и хранить ключевую информацию. В условиях постоянного развития технологий злоумышленники всё чаще используют атаки по сторонним каналам, позволяющие обойти традиционные механизмы защиты и получить доступ к секретным данным. Подобные атаки направлены на физические параметры работы микроконтроллера, включая потребляемую мощность, электромагнитное излучение и временные характеристики выполняемых операций [3]. При этом информация может распространяться не только по электромагнитному, но и по акустическому каналу – известны также исследования, объединяющие несколько физических каналов утечки [4, 5].

Одной из ключевых задач микроконтроллера в защищённых системах является выполнение операций аутентификации и криптографической обработки данных, включая генерацию и хранение секретных ключей. Реализация криптографических алгоритмов на аппаратном уровне может быть уязвима из-за особенностей конкретных микросхем и платформ, что создаёт предпосылки для применения дифференциального анализа мощности и других методов анализа побочных каналов. Для защиты обрабатываемой информации микроконтроллеры используют аппаратные и программные механизмы безопасности, включая защищённые области памяти, генераторы случайных чисел и маскирование промежуточных значений [6, 7]. Тем не менее, даже математически стойкие криптографические алгоритмы могут стать уязвимыми при неправильной реализации на уровне микроконтроллера, что также подчёркивает необходимость разработки методик оценки уязвимости микроконтроллеров к атакам по сторонним каналам.

Рост объёма конфиденциальной информации, обрабатываемой микроконтроллерами, усиливает значимость проблематики их защищённости. В последние годы наблюдается активное развитие методов атак по сторонним каналам, включая анализ потребляемой мощности и электромагнитного излучения. Эти методы позволяют восстановить секретные ключи и внутренние параметры алгоритмов, реализованных на микроконтроллерах, что делает их особенно опасными для систем безопасности.

Отдельное направление исследований связано с анализом угроз аппаратного уровня и моделированием сценариев атак на микроконтроллеры, включая сложные АРТ-атаки и использование программно-определяемых радиосистем (SDR) для регистрации сигналов. Технологический прогресс приводит к тому, что высокоточные средства анализа побочных каналов становятся доступными не только исследователям, но и злоумышленникам.

Электромагнитный (далее ЭМ) анализ основан на регистрации и анализе электромагнитного излучения, исходящего от работающего микроконтроллера – электрические устройства, обрабатывающие данные, излучают электромагнитные волны, содержащие информацию о выполняемых операциях, так как различные инструкции

и обработка различных данных приводят к различным паттернам электромагнитного излучения.

Электромагнитные атаки исторически требовали дорогостоящего специализированного оборудования: высокочувствительных датчиков, широкополосных усилителей, осциллографов высокого разрешения и мощных компьютеров для обработки сигналов. Стоимость подобной установки составляла десятки или сотни тысяч долларов, что делало электромагнитный анализ доступным только для крупных исследовательских центров и правительственных агентств. Появление программно-определяемых радиосистем расширило возможности регистрации и анализа сигналов без применения узкоспециализированного приёмного оборудования [8–10]. SDR-устройства, такие как «HackRF One», «USRP» (Universal Software Radio Peripheral) и «RTL-SDR», позволяют захватывать и анализировать широкий спектр радиочастот с помощью универсального аппаратного обеспечения и специализированного программного обеспечения.

Атаки по сторонним каналам довольно сложно предотвратить, так как они нацелены на конкретные реализации алгоритмов, а не на сами алгоритмы, что делает актуальной задачу разработки методов, ориентированных на оценку уязвимости конкретных микроконтроллерных платформ и реализаций протоколов. При этом для обеспечения комплексной защиты микроконтроллерных систем требуется учитывать как программные, так и аппаратные аспекты безопасности, включая архитектуру тестового доступа и интерфейсы диагностики, такие как стандарты «IEEE 1149.1» и «IEEE 1149.7» [11, 12].

В настоящей работе предложен метод оценки уязвимости микроконтроллеров к атакам по электромагнитному побочному каналу. Метод включает регистрацию излучения с помощью SDR-приёмника, предварительную обработку и выравнивание трасс, построение модели утечки по весу Хэмминга и корреляционное восстановление байтов ключа AES-128.

1. Математическая модель алгоритма

В рамках исследования реализуется атака с известным открытым текстом. Целевой микроконтроллер многократно выполняет криптографическую операцию шифрования блока данных алгоритмом AES-128 с фиксированным секретным ключом. В каждом из примерно 1000 независимых экспериментов на вход алгоритма подаются различные открытые данные, а SDR-устройство регистрирует соответствующий радиосигнал, излучаемый микроконтроллером во время выполнения операции. Для каждого эксперимента сохраняются открытый текст длиной 16 байт и соответствующая временная реализация ЭМ-сигнала (около 10 000 отсчётов за время выполнения одного цикла шифрования).

На рисунке 1 представлена общая архитектура системы анализа электромагнитного излучения микроконтроллера.

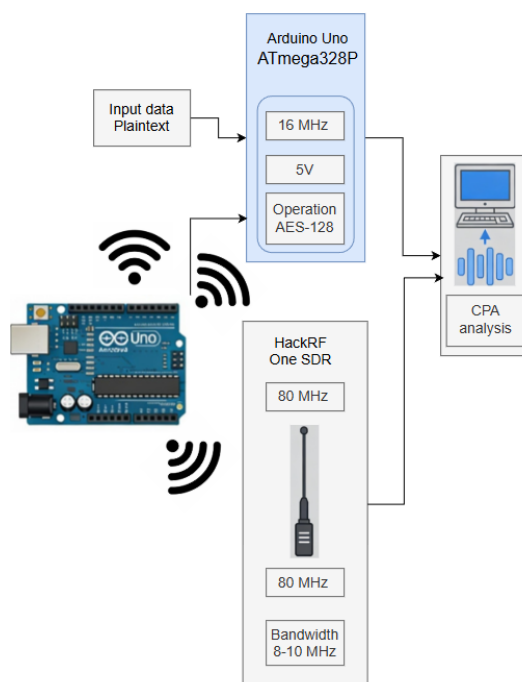


Рисунок 1 – Архитектура системы анализа

Система состоит из пяти основных компонентов: источника данных (открытые тексты), целевого устройства (Arduino с криптографической операцией), источника ЭМ-излучения, приёмника сигнала (HackRF One SDR) и компьютера для анализа данных.

Во время выполнения алгоритма AES внутри микроконтроллера вычисляются промежуточные значения, зависящие как от входных данных, так и от секретного ключа. В первом раунде байт открытого текста складывается по модулю 2 с соответствующим байтом ключа, после чего полученное значение преобразуется S-блоком (таблицей подстановки). Мощность электромагнитного излучения микроконтроллера в момент обработки этого значения коррелирует с его битовым содержанием: значения с большим количеством единиц в двоичном представлении потребляют больше энергии.

На рисунке 2 показан процесс формирования модели утечки: открытый текст побайтово объединяется с гипотезой ключа операцией XOR, результат подаётся на S-Box AES, где преобразуется в промежуточное значение – данное промежуточное значение представляется в двоичной форме, и подсчитывается количество единичных битов (вес Хэмминга) – именно это количество единиц предполагается коррелирующим с энергопотреблением микроконтроллера.

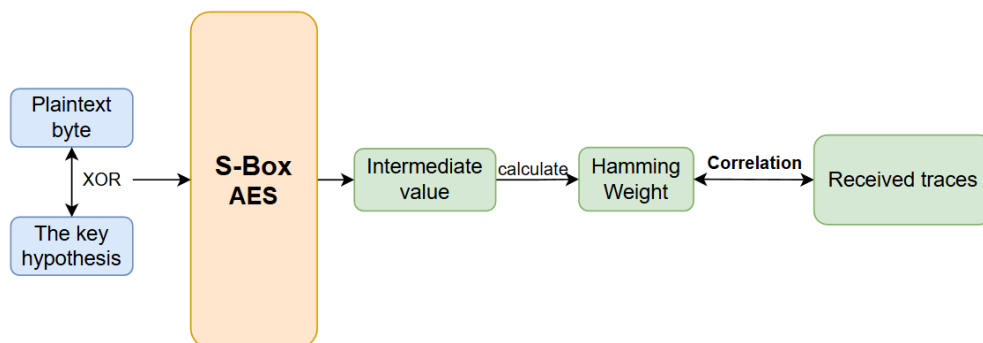


Рисунок 2 – Модель утечки

Предположим, что истинное значение ключевого байта нам неизвестно. В таком случае происходит перебор всех 256 возможных гипотез для этого байта, где для каждой

гипотезы ключа вычисляется математическое ожидание битового веса промежуточного значения на основе всех входных данных, после чего ожидаемое значение сравнивается со всеми зарегистрированными ЭМ-трассами и вычисляется корреляция между ними для каждого момента времени. При правильной гипотезе ключа корреляция является максимальной в момент времени, соответствующий выполнению операции на микроконтроллере. Для неправильных гипотез корреляция останется близкой к нулю. Таким образом, байт ключа восстанавливается по максимальному пику корреляции.

Основу статистической обработки составляет корреляционный анализ мощности (CPA), основанный на предположении, что энергопотребление микроконтроллера в определённые моменты времени коррелирует с промежуточными значениями, вычисляемыми в ходе криптографической операции [13]. Задача анализа состоит в том, чтобы перебрать все возможные значения ключевого байта (256 гипотез) и для каждой гипотезы вычислить статистическую корреляцию между предполагаемой утечкой информации и набором зарегистрированных ЭМ-трасс. Правильная гипотеза ключа должна демонстрировать более высокую корреляцию по сравнению со всеми неправильными гипотезами.

Для проведения CPA выбирается промежуточное значение, зависящее как от входных данных, так и от ключа. В рассматриваемом случае это выход S-блока в первом раунде алгоритма AES-128 после операции XOR входного байта с байтом ключа. Для каждой гипотезы k от 0 до 255 и каждого входного байта открытого текста d_i вычисляется промежуточное значение:

$$v_k^{(i)} = SBox[d_i \oplus k], \quad (1)$$

где $i = 1 \dots N$ – номер измерения (трассы).

На основе полученного промежуточного значения строится модель утечки в виде веса Хэмминга (количество единиц в двоичном представлении):

$$M_k^{(i)} = HW(v_k^{(i)}), \quad (2)$$

и так как $v_k^{(i)}$ – байт, то $M_k^{(i)} \in \{0, 1, \dots, 8\}$.

Коэффициент корреляции Пирсона между смоделированной утечкой и реальной мощностью для каждой гипотезы k и момента времени t вычисляется как

$$p_{k,t} = \frac{\sum_{i=1}^N (M_k^{(i)} - \bar{M}_k) \cdot (P_t^{(i)} - \bar{P}_t)}{\sqrt{\sum_{i=1}^N (M_k^{(i)} - \bar{M}_k)^2 \cdot \sum_{i=1}^N (P_t^{(i)} - \bar{P}_t)^2}}, \quad (3)$$

где $\bar{M}_k = \frac{1}{N} \sum_{i=1}^N M_k^{(i)}$ – среднее значение модели утечки для гипотезы k ;

$\bar{P}_t = \frac{1}{N} \sum_{i=1}^N P_t^{(i)}$ – среднее значение мощности в момент времени t .

Результатом является матрица размером $256 \times T$, где каждая строка соответствует одной гипотезе ключа, а каждый столбец – одному моменту времени.

Успешность CPA-атаки зависит от количества доступных трасс: при малом числе трасс (менее 100) статистический шум преобладает над полезным сигналом, и корреляция может быть неразборчивой. По мере увеличения количества трасс пик корреляции для правильного ключа становится всё более выраженным, а корреляции для неправильных гипотез остаются близки к нулю. В практических экспериментах на зашумленных SDR-системах с расстоянием 5–7 см до антенны требуется около 500–2000 трасс

для надёжного восстановления одного байта ключа. В рассматриваемом случае используется примерно 1000 трасс, что обеспечивает хороший баланс между достаточностью данных и практической осуществимостью сбора.

Поскольку ключ AES-128 состоит из 16 байт, корреляционный анализ выполняется отдельно для каждого из них: определяется временной интервал, в котором соответствующее промежуточное значение обрабатывается S-блоком – в результате восстанавливаются все 16 байтов секретного ключа.

2. Практические результаты

Эксперимент проводился с использованием метода SDR-атаки на микроконтроллер, представленного на рисунке 3.

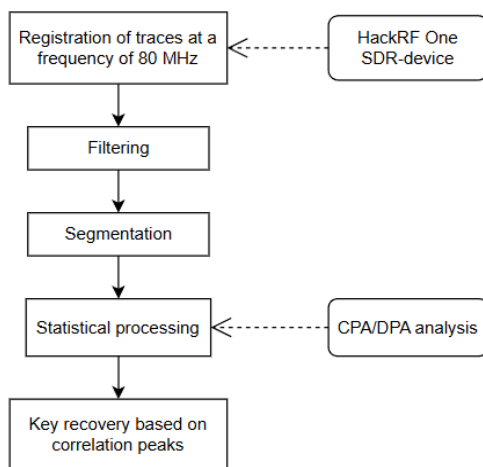


Рисунок 3 – Алгоритм SDR-атаки

Метод включал следующие шаги:

1) Захват сигнала: SDR-устройство подстраивается на частоту, излучаемую микроконтроллером, и регистрирует сигнал в течение всего времени выполнения криптографической операции. Частота может варьироваться в зависимости от конкретной архитектуры микроконтроллера и используемого кварцевого генератора, однако нередко находится в диапазоне от нескольких МГц до сотен МГц.

2) Предварительная обработка: захваченные сигналы проходят цифровую фильтрацию для удаления шума и помех, нормализацию амплитуды и синхронизацию с началом криптографической операции.

3) Сегментация и выравнивание: если проводится несколько записей одной и той же операции, то необходимо выравнивать трассы относительно друг друга для обеспечения точного сравнения.

4) Статистический анализ: применяется корреляционный анализ, анализ главных компонент (РСА) и другие статистические методы выявления паттернов, коррелирующих с обрабатываемыми данными или ключом.

5) Восстановление информации: на основе выявленных паттернов проводится проверка гипотез о значениях и восстановление промежуточных переменных или секретного ключа.

Для проведения атаки по перехвату и анализу электромагнитного излучения микроконтроллера была организована лабораторная установка, состоящая из следующих компонентов. В качестве целевого устройства использовалась плата «Arduino Uno» на базе

8-битного микроконтроллера «ATmega328P», работающего на тактовой частоте 16 МГц [14]. На данном микроконтроллере была реализована программа, выполняющая многократное шифрование блоков данных алгоритмом AES-128 с фиксированным секретным ключом. Для каждого цикла шифрования микроконтроллер получал от компьютера новый набор открытых данных по интерфейсу UART и передавал результат шифрования обратно без использования дополнительного шифрования на рассматриваемом уровне взаимодействия.

В качестве устройства захвата электромагнитного излучения была выбрана SDR-платформа «HackRF One», способная принимать сигналы в диапазоне частот от 1 МГц до 6 ГГц. Устройство «HackRF One» подключалось к персональному компьютеру через интерфейс USB, который обеспечивал как питание устройства, так и передачу цифровых отсчётов сигнала на компьютер для последующей обработки. Антенна, подключённая к «HackRF One», представляла собой монопольную антенну длиной примерно 15 см, оптимизированную для работы на частотах вблизи 80 МГц. Антенна была расположена на расстоянии 5–7 см от печатной платы Arduino, параллельно плоскости платы, что обеспечивало максимальный уровень сигнала при сохранении неинвазивного характера измерений.

Персональный компьютер, использовавшийся для управления экспериментом, имел процессор «Intel Core i5», 8 ГБ оперативной памяти и работал под управлением операционной системы Linux. На компьютер была установлена среда «GNU Radio Companion» для настройки параметров захвата HackRF, а также интерпретатор «Python 3» с необходимыми библиотеками (numpy, scipy, h5py) для последующей обработки и анализа данных.

Основные параметры захвата радиосигнала были установлены следующим образом. Центральная частота захвата установлена на уровне 80 МГц, что соответствует пятой гармонике тактовой частоты микроконтроллера ($16 \text{ МГц} \times 5$) – выбор данной частоты обусловлен тем, что электромагнитное излучение, генерируемое микроконтроллером при выполнении операций, содержит значительную энергию именно на гармониках тактовой частоты. Полоса пропускания приёмника была установлена на 2 МГц, что обеспечивает захват достаточного частотного диапазона без чрезмерного увеличения уровня шума. Частота дискретизации была установлена на уровне 10 миллионов отсчётов в секунду, что достаточно для разрешения по времени изменений сигнала в интервале 100 наносекунд – это соответствует нескольким циклам работы микроконтроллера на частоте 16 МГц.

На рисунке 4 проиллюстрированы несколько зарегистрированных трасс, демонстрирующих воспроизводимость электромагнитного излучения микроконтроллера.

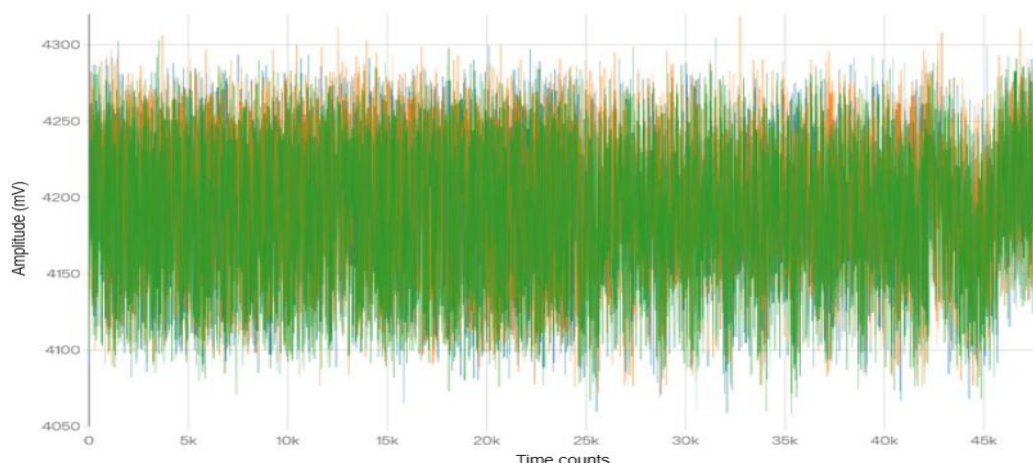


Рисунок 4 – Зарегистрированные ЕМ трассы

Для более детального анализа был выполнен спектральный анализ нескольких трасс. Применение дискретного преобразования Фурье к отсчётам ЭМ-сигнала позволило выявить, что основная энергия сигнала сконцентрирована на частотах в диапазоне 70–90 МГц, что соответствует ожиданиям для гармоник 16 МГц тактовой частоты. Спектральные компоненты вне рассматриваемого диапазона имели значительно меньшую амплитуду и отражали фоновый шум окружающей среды.

Также был оценён уровень шума в каждой трассе путём анализа дисперсии амплитуд в первых 100 отсчётах каждой трассы (до начала активной части шифрования). Средний уровень стандартного отклонения шума составил примерно 3–5 мВ, что было приемлемым для последующего анализа при условии использования достаточного количества трасс с целью усреднения и повышения отношения сигнал-шум.

На основе проведённого первичного анализа был сделан вывод о достаточном качестве собранного датасета для проведения корреляционного анализа мощности. Перехваченные трассы содержали выраженные пики, соответствующие выполнению криптографических операций, и низкий уровень помех, что обеспечивало благоприятные условия для восстановления секретного ключа.

На рисунке 5 представлен график корреляции во времени для одного байта ключа: по оси абсцисс отложен номер отсчета от 0 до 10000, по оси ординат – коэффициент корреляции от -1 до 1; 256 линий (по одной для каждой гипотезы ключа), одна из них с ярким пиком (правильный ключ), остальные близко к нулю.

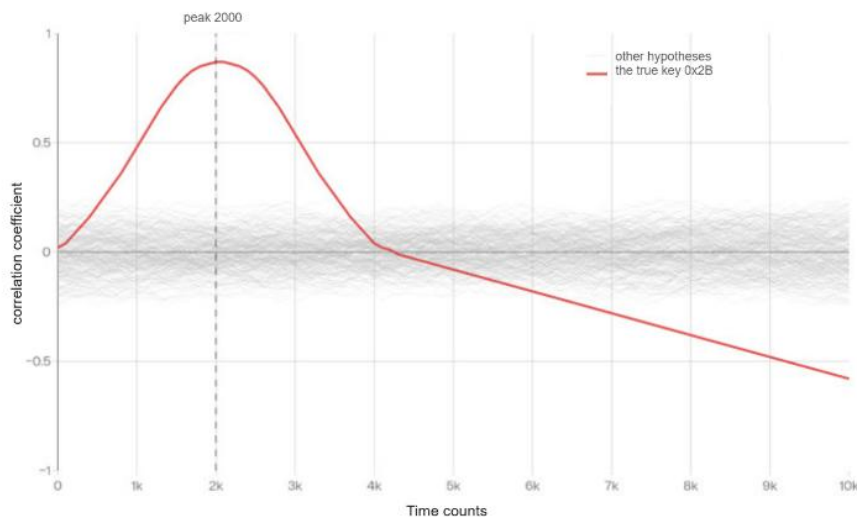


Рисунок 5 – Корреляционные зависимости для одного байта ключа

Результаты эксперимента показали успешное восстановление всех 16 байтов секретного ключа. В таблице 1 приведены восстановленные значения, а также максимальные коэффициенты корреляции, достигнутые для каждого байта.

Таблица 1 – Результат восстановления байтов ключа

Индекс байта	Восстановленное значение (hex)	Максимальная корреляция
0	2B	0,823
1	7E	0,756
2	15	0,841
3	A0	0,798
4	D4	0,812
5	39	0,769
6	86	0,834
7	F1	0,795
8	23	0,827
9	5C	0,789
10	B7	0,816
11	E2	0,804
12	61	0,835
13	4F	0,791
14	9A	0,823
15	C8	0,768

Проведённый эксперимент продемонстрировал возможность восстановления полного 128-битного ключа AES микроконтроллера «ATmega328P» через анализ электромагнитного излучения. Полученные результаты показывают:

- Успешность восстановления: все 16 байтов AES-128 ключа восстановлены;
- Количество требуемых трасс: 850-1200 трасс для коэффициента корреляции не менее 0,75;
- Средний коэффициент корреляции: 0,806 (диапазон: 0,756–0,841);
- Время анализа: 8–12 минут.

Заключение

В данной работе была выбрана атака на основе корреляционного анализа электромагнитного излучения, так как рассматриваемый подход эффективен против микроконтроллеров и других встраиваемых криптографических устройств. Атака по сторонним каналам основана на мониторинге изменений электромагнитного излучения устройства в процессе выполнения криптографических операций и анализе этих изменений для извлечения секретных ключей или другой конфиденциальной информации.

В результате исследования подтверждена возможность восстановления ключа AES-128, используемого микроконтроллером «ATmega328P» на плате «Arduino Uno», посредством корреляционного анализа электромагнитных трасс. С использованием модели утечки по весу Хэмминга были восстановлены все 16 байтов 128-битного ключа, а также разработан метод выявления уязвимостей микроконтроллеров к атакам по сторонним каналам на основе регистрации электромагнитного излучения. Полученные

результаты показывают, что исследованная реализация AES-128 уязвима к атакам по электромагнитному побочному каналу.

Благодарности

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-00003-24-01 от 08.02.2024 (проект FSEE-2024-0003).

Список литературы

1. Trifonov, V. E., Ponomareva, A. F., Levina, A. B., Krasov, K. S., Diaghilev, N. A., & Nemaltsev, D. A. (2025). Architectural vulnerabilities of IoT devices in the context of side channel attacks. In 2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), Antalya, Turkiye. 1–6, DOI: 10.1109/ACDSA65407.2025.11165979;
2. Akhmetvaleeva, L. V. (2024). Security of microcontrollers in embedded systems: threats and protection methods. *Economics and Management: Problems and Solutions*, 9/7(150), 4–11. DOI: 10.36871/ek.up.p.r.2024.09.07.001;
3. Kocher, P., Jaffe, J., Jun, B., & Rohatgi, P. (2011). Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1), 5–27, DOI: 10.1007/s13389-011-0006-y;
4. Genkin, D., Shamir, A., Tromer, E. (2014). RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In: *Advances in Cryptology. CRYPTO 2014. Lecture Notes in Computer Science*, 8616, Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-662-44371-2_25;
5. Krasov, K. S., & Levina, A. B. (2025). Algorithm for Combining Acoustic and Electromagnetic Channels to Perform an Attack on RSA Algorithm in the GnuPG Program. *Journal of Communications*, 20(6). DOI: 10.12720/jcm.20.6.724-730;
6. Abromeit, A. (2021). Automated masking of software implementations on industrial microcontrollers. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE). 1006–1011. IEEE. DOI: 10.23919/DAT51398.2021.9474183;
7. Басан, Е. С., Силин, О. И., Фирсова, М. Г. (2025). A methodology for selecting effective countermeasures to increase the fault tolerance of cyberphysical systems. *Вопросы кибербезопасности*, 1(65), 28–40. DOI: 10.21681/2311-3456-2025-1-28-40;
8. Буневич, М. А., Майоров, А. И., & Врублевский, И. А. (2023). Применение SDR-приемопередатчиков в системах для поиска закладных радиоустройств. *Цифровая трансформация*, 28(4), 62–71. DOI: 10.35596/1729-7648-2022-28-4-62-71;
9. Нанда, Ч. (2025). Применение цифрового радиоприемника Hack-RF One для обнаружения канала управления БПЛА. *Информационные системы и технологии: 61-я научная конференция аспирантов, магистрантов и студентов*. 123–125. URL: <https://libeldoc.bsuir.by/handle/123456789/60539>;
10. Морозова, А. И. (2025). Прием сигналов с использованием SDR-приемников. *Материалы XXI Всероссийской (национальной) научно-технической конференции студентов и аспирантов*. Екатеринбург. 588–593. URL: <https://elar.usfeu.ru/handle/123456789/13774>;
11. IEEE Standard for Test Access Port and Boundary-Scan Architecture. In IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001). 1–444. 2013. DOI: 10.1109/IEEESTD.2013.6515989;

12. IEEE Standard for Reduced-Pin and Enhanced-Functionality Test Access Port and Boundary-Scan Architecture. In IEEE Std 1149.7-2009. 1–985. 2010. DOI: 10.1109/IEEESTD.2010.5412866;
13. Lo, O., Buchanan, W. J., & Carson, D. (2017). Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). *Journal of Cyber Security Technology*, 1(2), 88–107. DOI: 10.1080/23742917.2016.1231523;
14. Banzi, M., & Shiloh, M. Getting Started with Arduino. Maker Media, CA: Sebastopol, 2018.