УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2019 Том 19 № 6 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTCS
November–December 2019 Vol. 19 No 6 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 004.056 doi: 10.17586/2226-1494-2019-19-6-1122-1129

ПОВЫШЕНИЕ УРОВНЯ РАСПОЗНАВАНИЯ УТЕЧЕК ИНФОРМАЦИИ ПО СТОРОННИМ КАНАЛАМ С ИСПОЛЬЗОВАНИЕМ ВЭЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

Д.М. Слепцова[a], А.Б. Левина[b]

[a] Riscure, Дельфт, 2628 XJ, Нидерланды
[b] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: levina@cit.ifmo.ru

Информация о статье
Поступила в редакцию 21.08.19, принята к печати 14.10.19
Язык статьи — русский

Ссылка для цитирования: Слепцова Д.М., Левина А.Б. Повышение уровня распознавания утечек информации по сторонним каналам с использованием вэйвлет-преобразования // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 6. С. 1122–1129. doi: 10.17586/2226-1494-2019-19-6-1122-1129

Аннотация

Предмет исследования. Представлены результаты экспериментального исследования влияния предобработки на основе вэйвлетного преобразования на величину статистической утечки информации в сигнале, полученном по сторонним каналам. Изучаемый сигнал получен по электромагнитному стороннему каналу с платы на базе процессора ARM-Cortex M4F. Съем сигнала произведен на расстояниях 1 мм и 3 см. Во время снятия сигнала на плате выполнялся алгоритм AES (Advanced Encryption Standard). **Метод.** Электромагнитный сигнал после снятия обрабатывается при помощи дискретного вэйвлет-преобразования со сжатием коэффициентов детализации. Исследовано влияние различных порогов сжатия, вэйвлет-функций, а также уровня вэйвлет-разложения сигнала. После обработки на записях сигнала проводится анализ утечек при помощи метода оценки утечки тестового вектора (TVLA), основанного на статистическом тесте Уэлча. Полученные оценки используются для сравнения вэйвлет-преобразования с оценкой утечки, проведенной на оригинальном сигнале. **Основные результаты.** Сигнал, обработанный при помощи вэйвлет-преобразования, показывает более высокие показатели статистического теста, что означает большую уверенность в наличии утечки информации. Универсальный порог и обнуление коэффициентов детализации увеличивают величину t-критерия в 1,4 раза. Третий уровень разложения показал наивысший результат для всех вэйвлет-функций. Дискретный вэйвлет Мейера показывает лучший результат во всех экспериментах, также стабильный результат в экспериментах показывают симлеты и коифлеты. **Практическая значимость.** Статистические методы, такие как статистический тест Уэлча, позволяют обнаруживать утечки без проведения дорогостоящих и трудоемких исследований и атак. Вэйвлет-преобразование и обработка полученного сигнала увеличивает информационные составляющие сигнала, что позволяет получить более близкие к реальным статистические профили сигналов. Вэйвлет-преобразование также позволяет находить утечки на меньшем количестве записей сигнала.

Ключевые слова
вэйвлет-преобразование, сторонние каналы, статистический тест Уэлча, электромагнитные утечки, пороговая фильтрация

doi: 10.17586/2226-1494-2019-19-6-1122-1129

SIDE-CHANNEL INFORMATION LEAK DETECTION WITH WAVELET TRANSFORMATION

D.M. Sleptsova[a], A.B. Levina[b]

[a] Riscure, Delft, 2628 XJ, The Netherlands
[b] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: levina@cit.ifmo.ru

Article info
Received 21.08.19, accepted 14.10.19
Article in Russian

For citation: Sleptsova D.M., Levina A.B. Side-channel information leak detection with wavelet transformation. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 6, pp. 1122–1129 (in Russian). doi: 10.17586/2226-1494-2019-19-6-1122-1129

Abstract

Subject of study. The paper presents the results of the experimental study of a wavelet-based pre-processing that was used to increase the amount of statistically-discoverable information leakage in a side-channel signal. The studied signal was acquired

via an electromagnetic channel of the ARM-Cortex M4F processor. The signal was recorded at the distance of 1 mm and 3 cm. During signal collection, the Advanced Encryption Standard (AES) algorithm was executed on the board. **Method.** After the acquisition, electromagnetic signal is processed using a discrete wavelet transform with shrinkage of the detail coefficients. The influence of various shrinkage thresholds, mother wavelet, and wavelet decomposition level is studied. After processing of the signal records, the leakage analysis is performed using the Test Vector Leakage Assessment (TVLA), a method based on the Welch statistical test. The obtained estimates are used to compare wavelet transform pre-processing with the leakage estimate of the original signal. **Main Results.** The signal processed by a wavelet transform shows higher values of the statistical test, that means more confidence in the presence of an information leakage. The universal threshold and zeroing detail coefficients increase the value of the t-criterion by 1.4 times. The third level of decomposition shows the highest result for all wavelet functions. The discrete wavelet of Meyer shows the best result in all experiments. Symlets and Coiflets also show stable results in the experiments. **Practical Relevance.** Statistical methods, such as the Welch statistical test, can detect leakage without costly and time-consuming stages such as research and attacks. The wavelet transform and processing of the received signal increases the informational components of the signal providing close-to-real statistical signal profiles. Pre-processing based on wavelet transform also allows for leakage detection on fewer signal records.

Keywords
wavelet transformation, side-channel analysis, Welch's t-test, electromagnetic leakage, thresholding

Введение

Впервые анализ криптоустройств к атакам по сторонним каналам был представлен в работе Пола Кохера [1] в 1996 г. В данной статье сторонним каналом для снятия секретной информации было время выполнения криптоопераций. Спустя несколько лет Кохер предложил еще одну атаку — атаку по потреблению энергии, известную как дифференциальный анализ мощности (DPA) [2]. Позже электромагнитный сигнал, полученный различными датчиками, был успешно использован в следующих работах [3–5]. Атаки по сторонним каналам, использующие как сторонний канал электромагнитный сигнал, называются дифференциальный электромагнитный анализ (DEMA). Эффективность DPA и DEMA была проверена на различных устройствах с использованием различных криптографических алгоритмов (DES, AES, RC4, ECC, RSA).

В связи с тем, что обнаружение информации основано на содержании сигнала, полученного по сторонним каналам, отношение сигнал/шум (ОСШ) может существенно влиять на точность полученных данных. Если уровень нежелательного шума чрезвычайно высок, то утечка может быть не обнаружена. Одним из способов уменьшения шума является усреднение записанного сигнала, как представлено в работах [2] и [6]. Однако этот метод требует большого количества сигналов, которые также должны быть выровнены по времени. Существует улучшение метода шаблонной атаки [6], основанное на создании точной модели шума в качестве шаблона, в дополнение к шаблону работы устройства. Несмотря на эффективность, данный способ работает лишь в случае шаблонной атаки, которая требует длительного сбора сигнала и профилирования устройства. Другими способами улучшения качества сигнала для обнаружения утечек являются кумулянт высокого порядка [7, 8] и фильтр Калмана [9, 10]. Кумулянт высокого порядка особенно эффективен при работе с гауссовским шумом, но процесс оценки кумулянта смешивает полезную информацию и приводит к ограниченным шумоподавляющим характеристикам. Использование фильтра Калмана усложняется необходимостью вычисления уравнения конкретного состояния и комплексной оценкой параметров.

Вэйвлет-преобразование несколько раз использовалось для изучения энергопотребления устройства [11–14]. Энергопотребление устройства — гораздо менее зашумленный канал, зачастую получаемый при модификации устройства, например, при удалении конденсаторов. К тому же атака по энергопотреблению требует внедрения щупа в микросхему, что делает компрометацию устройства в условиях реального мира дорогостоящей и заметной для пользователей устройств. Снятие утечки по электромагнитному каналу не оставляет следов и не требует модификации устройства, что делает этот сторонний канал практичным для реального атакующего, а значит, более опасным. Выявление угроз подобного рода является важным для производителей устройств. Вэйвлет-преобразование сигнала позволяет производить исследования и анализировать уязвимости электромагнитного стороннего канала с меньшими трудозатратами.

При изучении неизвестного сигнала проведение атаки является дорогостоящим процессом и требует длительного времени для нахождения уязвимостей. Одним из способов выявления утечки без проведения атаки является статистическое исследование сигнала. При помощи статистического исследования можно проверить гипотезу о принадлежности двух наборов записей сигнала со специально подобранными значениями к одному распределению. Статистический метод исследования не требует длительного анализа устройства и сигнала. В данной работе производится исследование статистических показателей утечки для сигнала, обработанного с помощью вэйвлет-преобразования.

Вэйвлет-преобразование и пороговое сжатие

Ограничения, существующие в преобразовании Фурье (ПФ), привели к возникновению вэйвлет-анализа. Вэйвлет-анализ в отличие от ПФ позволяет исследовать сигнал в частотной и временной области. Вэйвлет-преобразование гораздо эффективнее в работе с нестационарными сигналами, а современные реализации, основанные на квадратичных фильтр-банках, вычисляются быстрее, чем ПФ. В отличие

от синусоид ПФ вэйвлет-функция конечна, а ее амплитуда начинается с нуля, возрастает и снова убывает к нулю.

При анализе сигнала вэйвлет-преобразование позволяет сжимать энергию исходного сигнала в несколько значений высоких энергий (приближения). Добавленный шум преобразуется в значения низкой энергии (детали) и может быть отфильтрован.

Фильтрация значений детализации позволяет увеличить информационную составляющую сигнала и улучшить статистическое обнаружение информационных утечек в электромагнитном сигнале.

Помимо возможности создавать собственные вэйвлет-функции, существует несколько стандартных семейств, используемых в различных приложениях. Для данного исследования было выбрано несколько вэйвлет-семейств. Для сохранения энергии сигнала все выбранные вэйвлет-функции являются ортогональными. Количество ускользающих моментов обозначается в названии вэйвлета как N. Количество ускользающих моментов – один из основных параметров вэйвлет-функции, отражающий ее гладкость и количество сэмплов сигнала, которое использует функция для вэйвлет-преобразования в каждой временной точке. Для первоначального анализа выбрано несколько первичных ускользающих моментов, чтобы изучить зависимость между гладкостью вэйвлета и эффективностью сжатия. В данной работе были рассмотрены следующие вэйвлет-семейства.

1. Вэйвлет Хаара — самый простой из известных вэйвлетов, является набором ортогональных функций, которые не являются непрерывно дифференцируемыми. Также является вэйвлетом Добеши с одним ускользающим моментом (db1).

2. Вэйвлет Добеши (dbN). Вэйвлеты Добеши обеспечивают более эффективный анализ и синтез, чем вэйвлеты Хаара благодаря ортогональности и регулярности.

3. Вэйвлет коифлет (Coiflet) (coifN) имеет большую симметрию, чем dbN, и имеет такую же длину опоры с db3N.

4. Вэйвлет симлет (Symlet) является околосимметричной вэйвлет-функцией. Это улучшение вэйвлет-функции Добеши.

5. Дискретный вэйвлет Мейера – как ортогональный и симметричный вэйвлет часто используется для сжатия и удаления шума.

6. Биоортогональный (biorNr.Nd) вэйвлет, основной особенностью которого является линейная фаза, улучшающая реконструкцию изображения. Также количество ускользающих моментов восстанавливающей функции больше, чем в анализирующей функции, что может позволить восстановить более гладкий сигнал и уменьшить шумовую компоненту.

В данной работе для вычисления порогового значения сжатия использованы следующие методы:

— rigrsure — порог вычисляется на основе риска Штейна (SURE);

— minimaxi — порог с риском, соответствующим минимальной из максимальных квадратичных ошибок;

— universal — универсальный порог Донохо, зависящий только от размера вектора коэффициентов;

— обнуление — обнуление каждого коэффициента детализации.

Существует также эвристический вариант порога SURE, где при большой разреженности коэффициентов вместо порога SURE вычисляется универсальный порог. Эвристический порог SURE равен либо порогу SURE, либо универсальному порогу, в зависимости от характеристик сигнала. В связи с тем что порог SURE и универсальный изучены в работе в качестве самостоятельных порогов, эвристический порог не включен в работу.

Статистическое обнаружение угрозы по стороннему каналу

Оценка утечки тестового вектора (TVLA) [15] — прямое применение статистического теста Уэлча для проверки утечек или уязвимостей сторонних каналов. Статистический тест Уэлча проверяет, имеют ли два набора данных одинаковые средние значения, и успешно работает в случае, когда два набора данных имеют неодинаковые распределения. Методологию TVLA можно разделить на две разные категории: неспецифическая TVLA и специфическая TVLA. В обоих случаях необходимо записать два набора сигналов по сторонним каналам. В случае неспецифического TVLA один набор соответствует фиксированному ключу и фиксированным, специально подобранным открытым текстам, подаваемым на устройство, второй набор содержит записи сигнала, соответствующие одному и тому же фиксированному ключу и случайным открытым текстам. Ключ шифрования известен при проведении TVLA теста.

Фиксированный набор данных подбирается таким образом, чтобы получить фиксированное энергопотребление устройства на некотором известном этапе и сравнить его с обработкой случайных данных. В атаках по сторонним каналам вес Хэмминга используется для моделирования энергопотребления памяти. Перед записью исследуемого параметра в память, значения ячеек памяти обнуляются, после чего производится запись параметра. Энергопотребление устройства будет равно количеству переходов из 0 в 1, что соответствует весу Хэмминга.

В рамках эксперимента известен ключ и подбираются открытые тексты, что позволяет предварительно вычислить результат шифрования и промежуточные значения алгоритма. Это позволяет получить

два разных набора записей сигнала: *A* (фиксированное промежуточное значение энергопотребление) и *B* (случайное промежуточное значение энергопотребления).

После этого проверка гипотезы осуществляется путем принятия нулевой гипотезы о том, что два набора записей сигнала имеют идентичные средние значения и дисперсию. Если нулевая гипотеза принята, это означает, что сигнал не содержит конфиденциальную информацию. С другой стороны, невыполненная нулевая гипотеза указывает на наличие утечки в сигнале. Это может быть выражено как:

$$TVLA = \frac{X_A - X_B}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}},$$

где N_A, N_B обозначают количество записей сигнала для наборов A и B соответственно. Среднее значение и стандартное отклонение случайного набора данных обозначаются как X_B и S_B. Точно также X_A и S_A означает среднее значение и стандартное отклонение фиксированного набора данных.

Нулевая гипотеза о двух равных средних отклоняется, когда t-критерий превышает пороговое значение ±4,5 стандартных отклонения, что обеспечивает степени свободы более 1000, $P[|TVLA| > 4{,}5] < 0{,}00001$. Как указано в вычисленных требованиях к эксперименту для AES (DTR, Derived Test Requirements) [16], использование порога ±4,5 приводит к уровню достоверности проведенных экспериментов 99,999 %. При преодолении t-критерием порога ±4,5 можно с 99,999 % достоверностью сказать, что два распределения имеют разные средние значения и дисперсию.

Таким образом, если значение TVLA находится в пределах ± 4,5, то считается, что сигнал не содержит утечку, зависящую от данных. Зависимость от данных выражается в том, что данные в фиксированном наборе подбираются так, чтобы промежуточные значения алгоритма имели фиксированный вес Хэмминга. Случайные данные будут иметь случайный вес Хэмминга. В случае, когда значение TVLA выходит за пределы порога ±4,5, нулевая гипотеза отвергается, и это означает, что существует утечка, пригодная для получения информации через сторонние каналы.

В данной работе исследования проводились на алгоритме AES-128. Смещение веса Хэмминга производилось в промежуточном результате шифрования State на пятом раунде шифрования при помощи программного обеспечения, которое подавало специально подобранные открытые тексты при известном фиксированном ключе шифрования. Это позволило подобрать открытые тексты таким образом, что вес Хэмминга был равен 4 для параметра State алгоритма AES-128. Полученные таким образом записи сигнала составляют фиксированный набор. Случайный набор данных содержит записи сигнала вне зависимости от веса Хэмминга промежуточного параметра State. Электромагнитный сигнал снимался во время выполнения процессором операции шифрования.

Метод обработки сигнала при помощи вэйвлет-преобразования и сжатия вэйвлет-коэффициентов

В рамках работы были произведены эксперименты на плате на базе процессора ARM-Cortex M4F. Во время выполнения процессором шифрования AES снимался электромагнитный сигнал на расстоянии 1 мм и 3 см. После записи полученный сигнал был обработан с помощью вэйвлетного сжатия, для улучшения качества сигнала были выполнены следующие действия.

1. Построение дискретного разложения с выбранным материнским вэйвлетом на нескольких уровнях k. Результатом первого шага является несколько векторов коэффициентов. Один вектор содержит низкочастотный сигнал и называется аппроксимацией, остальные k векторов содержат высокочастотный сигнал и называются коэффициентами детализации. Результатом вэйвлет-преобразования является значение «корреляции» вэйвлет-функции с сигналом в определенной временной точке. Чем выше получившийся коэффициент, тем более схожа вэйвлет-функция с сигналом в данной временной точке.

2. Оценка стандартного отклонения шума в векторе высокочастотной составляющей сигнала вычисляется по следующей формуле [17]:

$$\sigma_{mad} = \frac{median\left\{ \left|d_0\right|, \left|d_1\right|, \ \ldots \ \left|d_{2^{N-1}-1}\right| \right\}}{0{,}6745},$$

где d — это значения коэффициентов детализации, N — количество точек при дискретизации снятого электромагнитного сигнала.

3. Вычисление порога с использованием оценки, произведенной на шаге 2. Порог вычислялся с помощью 4 методов. λ — порог, используемый в вэйвлет-сжатии.

1) Универсальный порог:

$$\lambda_{universal} = \sqrt{2\ln(N)}.$$

2) Минимаксный порог, заданный в зависимости от количества точек в сигнале N:

$$\lambda_{minimaxi} = \begin{cases} (0{,}3936 + 0{,}10829 \log_2 N), & N > 32 \\ 0, & N \leq 32 \end{cases}.$$

3) Rigrsure, основанный на несмещенной оценке риска Штейна.

$$\lambda_{SURE} = \operatorname{argmin}_{\lambda \geq 0} SURE(\lambda, d)$$

$$SURE(\lambda, d) = N - 2 \cdot \#\{i : |d_i| \leq \lambda\} + \sum_{i=1}^{N} \min\left(|d_i|, \lambda\right)^2.$$

4) Heursure, являющийся комбинацией универсального и Rigrsure порогов.

$$\lambda_{heursure} = \begin{cases} \lambda_{universal}, & A < B \\ \min(\lambda_{universal}, \lambda_{SURE}), & A \geq B \end{cases},$$

где $A = \dfrac{\sum_{i=1}^{N} d_i^2}{N}$ и $B = 1 + \dfrac{\log_2 N^{3/2}}{\sqrt{N}}$.

В случае $A < B$ в качестве порога используется универсальный порог, в остальных случаях в качестве порога выбирается минимум из универсального порога и порога rigrsure.

4. Сжатие высокочастотного сигнала в форме коэффициентов с применением порогового значения.

Сжатие производится с применением «мягкого подхода». В данном подходе значения данных с абсолютным значением меньше порога заменяются на ноль. Значения данных с абсолютным значением, большим или равным значению порогового значения, сокращаются до нуля на пороговое значение. Новое значение коэффициента d' после применения порога λ к значению коэффициента d вычисляется следующим образом:

$$d' = \begin{cases} 0, & для\ |d| \leq \lambda \\ d - \lambda, & для\ d > \lambda \\ d + \lambda, & для\ d < -\lambda \end{cases}.$$

5. Восстановление сигнала при помощи обратного дискретного вэйвлет-преобразования (IDWT) вэйвлет-коэффициентов на всех частотах.

Дополнительные эксперименты были проведены с использованием обнуления коэффициентов вместо вычисления порога (шаг 2 и 3).

Использовано минимальное количество записей сигнала, необходимое для выполнения статистического теста – 1000 записей для каждого набора данных.

Для каждого набора данных был вычислен статистический тест Уэлча. Тест Уэлча выполняется для каждого записанного сигнала, поэтому в качестве результирующего значения было взято максимальное значение среди всех вычисленных.

Результаты

Вэйвлет-преобразование позволило диагностировать наличие утечки информации по стороннему каналу в 1,4 раза чаще по сравнению с проведением теста на оригинальных записях сигнала, не обработанных при помощи вэйвлет-преобразования. На рис. 1–3 представлены все исследованные вэйвлет-семейства и уровень разложения сигнала. Значение t-критерия для оригинальных записей сигнала равно 17,06 стандартных отклонений. На графиках оно обозначено красной линией для сравнения с записями сигнала, обработанными вэйвлет-преобразованиями. Желтым цветом показаны максимальные значения t-критерия для каждого набора вэйвлет-функций и уровней разложения. Повышение уровня разложения положительно сказалось на качестве выявления утечки. Количество ускользающих моментов незначительно влияет на результат преобразования, гораздо большую роль играет выбранная вэйвлет-функция. Наилучшие результаты показали коифлеты и дискретный вэйвлет Мейера. Порог rigrsure показал низкие результаты — для разреженного сигнала он оказался слишком мал и поэтому сигнал после сжатия оказался близок к оригинальному сигналу.

На рис. 4 показан график более зашумленного сигнала, снятого на расстоянии 3 см. Несмотря на значительную зашумленность данного сигнала, вэйвлет-преобразование позволило увеличить уверенность в наличии утечки на 10 %. Ведущими функциями также являются коифлеты и дискретный вэйвлет Мейера.

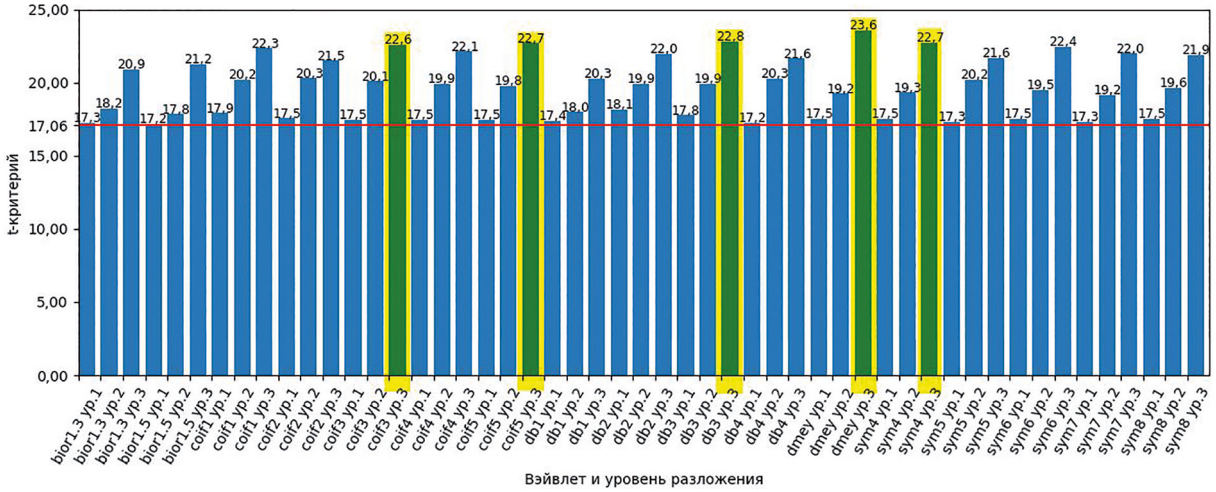

Рис. 1. t-критерий Уэлча для сигнала после вэйвлет-преобразования с обнулением коэффициентов детализации

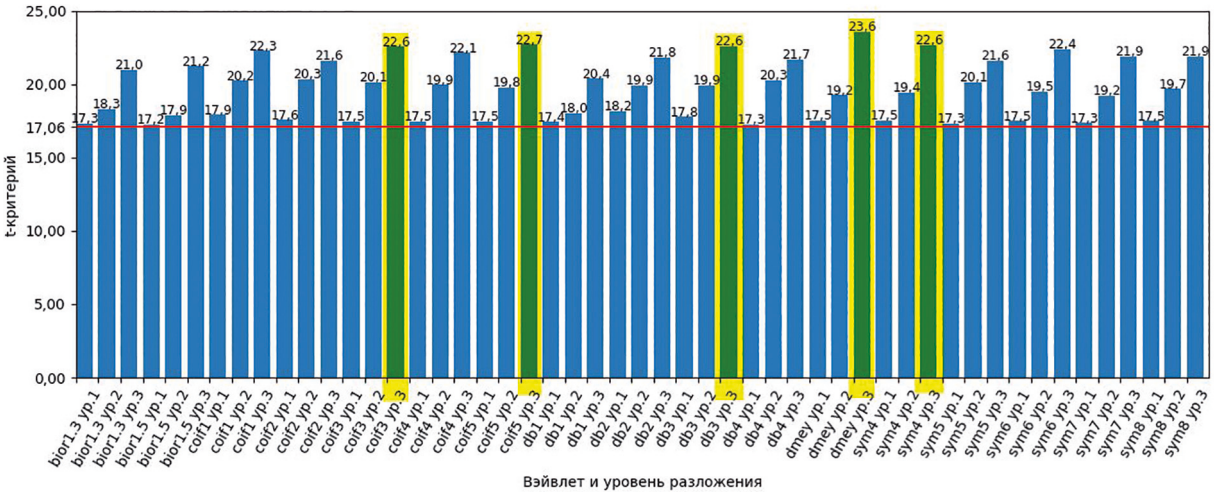

Рис. 2. t-критерий Уэлча для сигнала после вэйвлет-преобразования с универсальным порогом

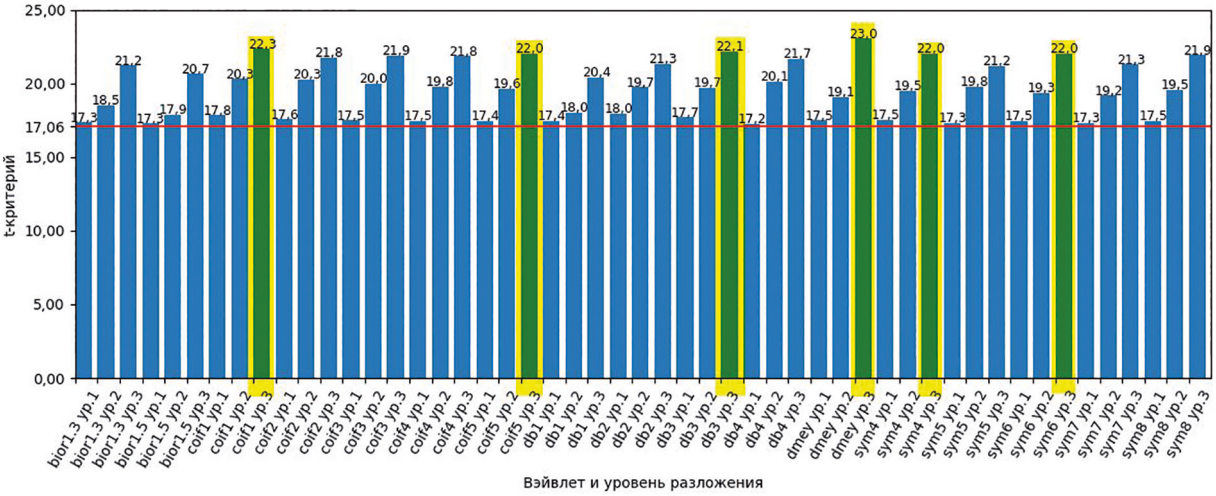

Рис. 3. t-критерий Уэлча для сигнала после вэйвлет-преобразования с минимаксным порогом

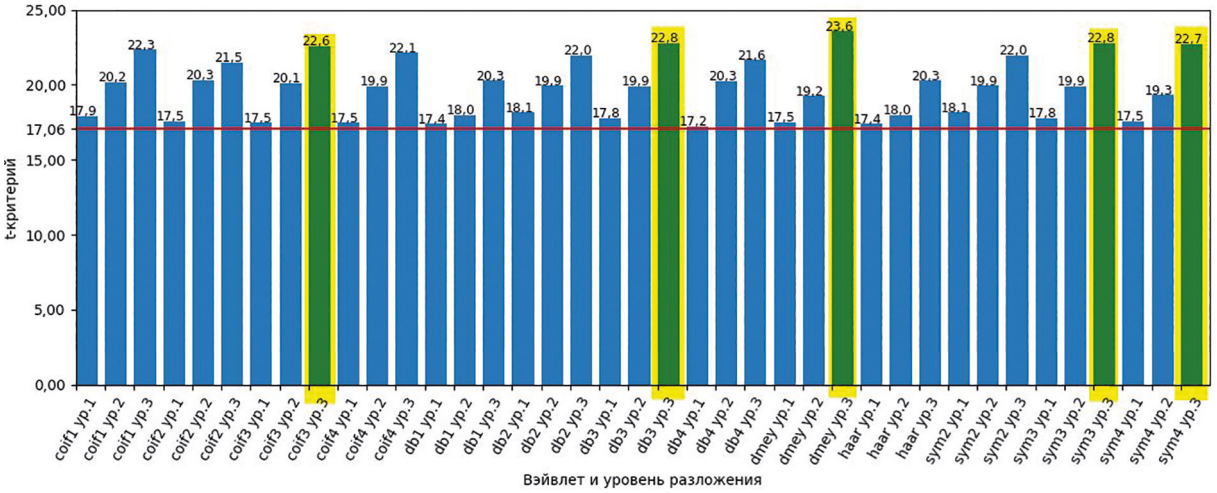

Рис. 4. t-критерий Уэлча для сигнала, снятого на расстоянии 3 см, после вэйвлет-преобразования с обнулением коэффициентов детализации

Заключение

В работе исследовано пять вэйвлет-семейств — биортогональные вэйвлеты, коифлеты, вэйвлеты Добеши, дискретный вэйвлет Мейера, симлеты. Дискретный вэйвлет Мейера позволяет получить наибольшее увеличение t-критерия. Методы определения порога сжатия вэйвлет-коэффициентов показывают одинаковое увеличение утечки, кроме порога rigrsure, при котором обработанный и оригинальный сигнал не отличаются.

Вэйвлет-преобразование позволяет обнаруживать утечки по стороннему каналу со значительно большей степенью уверенности — t-критерий Уэлча увеличивается в 1,4 раза. Выполнение преобразования и статистического теста не занимает значительного времени по сравнению с полноценной атакой и позволяет выявить утечку на этапе проектирования, или при вводе устройства в эксплуатацию в информационных системах.

Интересной областью для дальнейших исследований остается изучение устройств и нахождение эксплуатируемых угроз, позволяющих провести атаки по стороннему каналу для получения конфиденциальной информации. Утечка по стороннему каналу позволяет показать зависимость энергопотребления от обрабатываемых данных. В рамках обнаружения утечки вэйвлет-преобразование улучшает качество сигнала. Вэйвлет-преобразование может позволить обнаружить эксплатируемую угрозу с меньшим количеством записей сигнала.

Литература

1. Kocher P. Timing attack on implementation of Diffie-Hellman, RSA, DSS and other systems // Lecture Notes in Computer Science. 1996. V. 1109. P. 104–113.
2. Kocher P., Jaffe J., Jun B. Differential power analysis // Lecture Notes in Computer Science. 1999. V. 1666. P. 388–397.
3. Gandolfi K., Mourtel C., Olivier F. Electromagnetic attacks: concrete results // Proc. CHES. Paris, France. 2001. P. 252–261.
4. Quisquater J-J., Samyde D. Electromagnetic analysis (EMA): Measures and countermeasures for smart cards // Lecture Notes in Computer Science. 2001. V. 2140. P. 200–210.
5. Rao J.R., Rohatgi P. EMpowering side-channel attacks [Электронный ресурс]. URL: https://eprint.iacr.org/2001/037.pdf, свободный. Яз. англ. (дата обращения: 06.08.2019).
6. Chari A., Rao J.R., Rohatgi P. Template attacks // Lecture Notes in Computer Science. 2002. V. 2523. P. 13–28. doi: 10.1007/3-540-36400-5_3
7. Le T.-H., Clédière J., Servière C., Lacoume J.-L. Noise reduction in side channel attack using fourth-order cumulant // IEEE Transactions on Information Forensics and Security. 2007. V. 2. N 4. P. 710–720. doi: 10.1109/TIFS.2007.910252
8. Le T.-H., Clédière J., Servière C., Lacoume J.-L. How can signal processing benefit side channel attacks? // Proc. Workshop on Signal Processing Applications for Public Security and Forensics. (SAFE'07). 2007. P. 4218943.

References

1. Kocher P. Timing attack on implementation of Diffie-Hellman, RSA, DSS and other systems. *Lecture Notes in Computer Science*, 1996, vol. 1109, pp. 104–113.
2. Kocher P., Jaffe J., Jun B. Differential power analysis. *Lecture Notes in Computer Science*, 1999, pp. 388–397.
3. Gandolfi K., Mourtel C., Olivier F. Electromagnetic attacks: concrete results. *Proc. CHES. Paris, France*, 2001, pp. 252–261.
4. Quisquater J-J., Samyde D. Electromagnetic Analysis (EMA): Measures and countermeasures for smart cards. *Lecture Notes in Computer Science*, 2001, vol. 2140, pp. 200–210.
5. Rao J.R., Rohatgi P. *EMpowering side-channel attacks*. Available at: https://eprint.iacr.org/2001/037.pdf (accessed: 06.08.2019).
6. Chari A., Rao J.R., Rohatgi P. Template attacks. *Lecture Notes in Computer Science*, 2002, vol. 2523, pp. 13–28. doi: 10.1007/3-540-36400-5_3
7. Le T.-H., Clédière J., Servière C., Lacoume J.-L. Noise reduction in side channel attack using fourth-order cumulant. *IEEE Transactions on Information Forensics and Security*, 2007, vol. 2, no. 4, pp. 710–720. doi: 10.1109/TIFS.2007.910252
8. Le T.-H., Clédière J., Servière C., Lacoume J.-L. How can signal processing benefit side channel attacks? *Proc. Workshop on Signal Processing Applications for Public Security and Forensics. (SAFE'07)*, 2007, pp. 4218943.
9. Souissi Y., Danger J.-L., Mekki S., Guilley S., Nassar M. Techniques for electromagnetic attacks enhancement. *Proc. 5th*

9. Souissi Y., Danger J.-L., Mekki S., Guilley S., Nassar M. Techniques for electromagnetic attacks enhancement // Proc. 5th International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS 2010). 2010. P. 5487590. doi: 10.1109/DTIS.2010.5487590
10. Souissi Y., Guilley S., Danger J.-L., Mekki S., Duc G. Improvement of power analysis attacks using Kalman filter // Proc. IEEE International Coriference on Acoustics, Speech and Signal Processing (ICASSP 2010). 2010. P. 1778–1781. doi: 10.1109/ICASSP.2010.5495428
11. Charvet X., Pelletier H. Improving the DPA attack using Wavelet transform [Электронный ресурс]. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.6813&rep=rep1&type=pdf, свободный. Яз. англ. (дата обращения: 06.08.2019)
12. Li J., Li S., Shi Y., Zhou E. Wavelet de-noising method in the side-channel attack // Proc. 5th IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). 2015. P. 7338933. doi: 10.1109/ICSPCC.2015.7338933
13. Ai J., Wang Z., Zhou X., Ou C. Improved wavelet transform for noise reduction in power analysis attacks // Proc. 2016 IEEE International Conference on Signal and Image Processing (ICSIP). 2016. P. 602–606. doi: 10.1109/SIPROCESS.2016.7888333
14. Park A., Han D.-G., Ryoo J. CPA performance comparison based on Wavelet Transform // Proc. 46th IEEE International Carnahan Conference on Security Technology (ICCST). 2012. P. 201–206. doi: 10.1109/CCST.2012.6393559
15. Goodwill G., Jun B., Jaffe J., Rohatgi P. A testing methodology for sidechannel resistance validation [Электронный ресурс]. URL: https://csrc.nist.gov/csrc/media/events/non-invasive-attack-testing-workshop/documents/08_goodwill.pdf, свободный. Яз. англ. (дата обращения: 06.08.2019)
16. Test Vector Leakage Assessment (TVLA) Derived Test Requirements (DTR) with AES [Электронный ресурс]. URL: https://www.rambus.com/wp-content/uploads/2015/08/TVLA-DTR-with-AES.pdf, свободный. Яз. англ. (дата обращения: 12.10.2019).
17. Silverman B.W. Wavelets in statistics: beyond the standard assumptions [Электронный ресурс]. URL: http://doi.org/10.1098/rsta.1999.0442, ограниченный. Яз. англ. (дата обращения: 22.09.2019)

International Conference on Design and Technology of Integrated Systems in Nanoscale Era (DTIS 2010), 2010, pp. 5487590. doi: 10.1109/DTIS.2010.5487590
10. Souissi Y., Guilley S., Danger J.-L., Mekki S., Duc G. Improvement of power analysis attacks using Kalman filter. *Proc. IEEE International Coriference on Acoustics, Speech and Signal Processing (ICASSP 2010)*, 2010, pp. 1778–1781. doi: 10.1109/ICASSP.2010.5495428
11. Charvet X., Pelletier H. *Improving the DPA attack using Wavelet transform*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.6813&rep=rep1&type=pdf (accessed: 06.08.2019)
12. Li J., Li S., Shi Y., Zhou E. Wavelet de-noising method in the side-channel attack. *Proc. 5th IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC),* 2015, P. 7338933. doi: 10.1109/ICSPCC.2015.7338933
13. Ai J., Wang Z., Zhou X., Ou C. Improved wavelet transform for noise reduction in power analysis attacks. *Proc. 2016 IEEE International Conference on Signal and Image Processing (ICSIP)*, 2016, pp. 602–606. doi: 10.1109/SIPROCESS.2016.7888333
14. Park A., Han D.-G., Ryoo J. CPA performance comparison based on Wavelet Transform. *Proc. 46th IEEE International Carnahan Conference on Security Technology (ICCST)*, 2012, pp. 201–206. doi: 10.1109/CCST.2012.6393559
15. Goodwill G., Jun B., Jaffe J., Rohatgi P. *A testing methodology for sidechannel resistance validation*. Available at: https://csrc.nist.gov/csrc/media/events/non-invasive-attack-testing-workshop/documents/08_goodwill.pdf (accessed: 06.08.2019)
16. *Test Vector Leakage Assessment (TVLA) Derived Test Requirements (DTR) with AES*. Available at: https://www.rambus.com/wp-content/uploads/2015/08/TVLA-DTR-with-AES.pdf (accessed: 12.10.2019).
17. Silverman B.W. *Wavelets in statistics: beyond the standard assumptions*. Available at: http://doi.org/10.1098/rsta.1999.0442 (accessed: 22.09.2019)

Авторы

Слепцова Дарья Максимовна — аналитик-стажер, Riscure, Дельфт, 2628 XJ, Нидерланды, Scopus ID: 57191241688, ORCID ID: 0000-0001-6695-8068, dsleptsova@itmo.ru
Левина Алла Борисовна — кандидат физико-математических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56427692900, ORCID ID: 0000-0003-4421-2411, levina@cit.ifmo.ru

Authors

Daria M. Sleptsova — Security Analyst Intern, Riscure, Delft, 2628 XJ, The Netherlands, Scopus ID: 57191241688, ORCID ID: 0000-0001-6695-8068, dsleptsova@itmo.ru
Alla B. Levina — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56427692900, ORCID ID: 0000-0003-4421-2411, levina@cit.ifmo.ru