УДК 004.056 DOI 10.18522/2311-3103-2024-5-163-173

В.О. Малявина, Е.А. Маро

МОДЕЛИРОВАНИЕ УТЕЧЕК ПО ПОБОЧНЫМ КАНАЛАМ ДЛЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМОВ «МАГМА» И «КУЗНЕЧИК» НА ОСНОВЕ ЭМУЛЯТОРА ELMO

Анализ стойкости реализаций средств защиты информации к атакам по побочным каналам является актуальной задачей при разработке криптографических модулей. Первым этапом в исследовании стойкости по побочным каналам рассматривается оценка наличия статистических утечек в различных параметрах работы устройств в ходе выполнения криптографических алгоритмов. Универсальным источником, оцениваемым как побочный канал, рассматривается анализ энергопотребления устройства в ходе криптографических вычислений. В исследовательской работе с помощью инструмента ELMO получены трассы энергопотребления для алгоритмов шифрования «Магма» и «Кузнечик», выявлены инструкции, содержащие статистические утечки по энергопотреблению для исследуемых алгоритмов. Для моделирования трасс энергопотребления в ELMO реализован на языке С алгоритм шифрования ГОСТ Р 34.12—2015 (n=64 «Магма» и n=128 «Кузнечик»). Полнораундовая версия алгоритмов шифрования «Магма» и «Кузнечик» составляет соответственно 15400 инструкций (из них 4450 инструкций содержит потенциальную утечку по энергопотреблению) и 7167 инструкций (из них 4833 инструкций содержит потенциальную утечку по энергопотреблению). Выявление побочного канала (соответствующего обрабатываемым данным) может быть осуществлено с помощью статистического t-теста. Для выполнения этой задачи формируются два независимых набора трасс энергопотребления устройств: трассы при фиксированном значении входных векторов и трассы при произвольных (не совпадающих с фиксированными) значениях входных векторов. Выполнено моделирование утечек по энергопотреблению для различного числа раундов шифрования «Магма» и «Кузнечик» на о снове статистического t-теста. Определены инструкции, содержащие наибольшую статистическую зависимость на базе проведенного тестирования. Для шифра Магма выделены инструкции adds r3,r4,r3 и ldrb r3,[r3,r1], для шифра Кузнечик - lsls r5,r3,#0x0 и str r7,[r3,#0x20000888]. Выявленные инструкции являются оптимальными для последующего проведения дифференциальных или корреляционных атак по энергопотреблению на исследуемые алгоритмы шифрования.

Моделирование утечек по энергопотреблению; эмулятор ELMO; симметричный блочный алгоритм шифрования; ГОСТ Р 34.12-2015; шифр «Магма»; шифр «Кузнечик».

V.O. Malyavina, E.A. Maro

MODELING SIDE-CHANNEL LEAKAGES FOR THE CRYPTOGRAPHIC ALGORITHMS "MAGMA" AND "KUZNACHIK" BASED ON THE ELMO EMULATOR

Analysis of the resistance of implementations of information security tools to attacks via side channels is a relevant task in the development of cryptographic modules. The first stage in the study of resistance via side channels is the assessment of the presence of statistical leaks in various parameters of the operation of devices during the execution of cryptographic algorithms. The universal source, assessed as a side channel, is the analysis of the energy consumption of the device during cryptographic operations. In this research the ELMO tool was used to obtain power consumption traces for the Magma and Kuznyechik encryption algorithms, identify instructions containing statistical power consumption leaks for observed algorithms. To model the power consumption traces, the GOST R 34.12—2015 encryption algorithm (n=64 Magma and n=128 Kuznyechik) was implemented in C in ELMO. The full-round version of the Magma and Kuznechik encryption algorithms consists of 15,400 instructions (of which 4,450 instructions contain a potential leakage in energy consumption) and 7,167 instructions (of which 4,833 instructions contain a potential leakage in energy consumption), respectively. The side channel (corresponding to the processed data) can be identified using a statistical t-test. To perform this task, two independent sets of device energy consumption traces are formed: traces with a fixed value of the input vectors and traces with arbitrary (not coinciding with the fixed) values of the input vectors. Power consumption leaks were modeled for different numbers of Magma and Kuznyechik encryption rounds based on the statistical t-test. The identified instructions are optimal for subsequent differential or correlation attacks on power consumption on the observed encryption algorithms. The instructions containing the maximal statistical de-

pendence based on the conducted testing were determined. For the Magma cipher, the instructions added r3,r4,r3 and ldrb r3,[r3,r1] were identified, for the Kuznyechik cipher - lsls r5,r3,#0x0 and str r7,[r3,#0x20000888]. The identified instructions are optimal for subsequent differential or correlation attacks on power consumption on the encryption algorithms under research.

Power consumption leak modeling; ELMO emulator; symmetric block encryption algorithm; GOST R 34.12-2015; Magma cipher; Kuznyechik cipher.

Введение. Классический криптоанализ симметричных шифров рассматривает криптосистему как математический алгоритм, преобразующий некоторый входной текст (или наборы входных текстов) в выходной текст (соответствующий набор выходных текстов) на основе исследователь имеет полное описание преобразований, происходящих внутри криптосистемы, владеет зашифрованными текстами, может обладать соответствующими открытыми текстами (или их частями), но не обладает информацией об используемом секретном ключе. Классические методы криптоанализа опираются на использование недостатков математической конструкции шифра для вычисления ключа шифрования по известным данным, вычислительно быстрее полного перебора множества возможных значений ключей.

На практике криптографический алгоритм не ограничивается только математическим описанием алгоритма шифрования, так как не может существовать без физической реализации в виде конкретного программного или программно-аппаратного средства. Криптографический алгоритм разработан в определенной программной среде, реализуется на определенном оборудовании (типе процессора), что отражается на специфике работы криптосредства и может быть использовано исследователем при криптоанализе.

Атаки по побочным каналам. Атаки по побочным каналам представляют собой класс атак, направленный на использование уязвимости (недостатка) в практической реализации криптосистемы. Учитывая важность анализа безопасности различных реализаций криптографических систем, следует отдельно рассматривать стойкость средства защиты информации к атакам по побочным каналам [1–5]. Классификация атак по побочным каналам [6] приведена на рис. 1.

Первоначальным этапом оценки стойкости реализаций криптографических средств защиты к атакам по побочным каналам является выявление утечки, присущей работе криптосистемы. Одним из универсальных каналов утечки для криптографических систем служит канал энергопотребления. Атака по энергопотреблению — пассивная атака, направленная на выявление зависимости между энергопотреблением шифратора (процессора) и преобразуемыми данными с целью получения секретного ключа или защищаемой информации. При проведении атаки по энергопотреблению исследователь должен иметь возможность выполнять измерения энергопотребления с высокой точностью для получения информации о выполняемых на устройстве операциях и их параметрах. Типичная схема стенда для проведения атаки по энергопотреблению показана на рис. 2. Выделяют следующие разновидности атак, в которых используется информация об энергопотреблении: простой анализ энергопотребления [7, 8], дифференциальный анализ энергопотребления [9–11], корреляционный анализа энергопотребления [12–14] и анализ на основе шаблонов [15].

Стойкость реализации к утечкам по энергопотреблению рассматривается как важная составляющая обеспечения заданного уровня безопасности и доверия к средству защиты информации в целом.

В данном исследовании проведено моделирование трасс энергопотребления криптографических средств защиты информации, в основе которых используется реализация алгоритма ГОСТ Р 34.15-2015 [16] (n=64 «Магма»), и выполнен поиск наличия каналов утечки, путем выявления наборов инструкций, для которых имеются статистические зависимости энергопотребления устройства от значения обрабатываемых данных (по результатам t-теста).

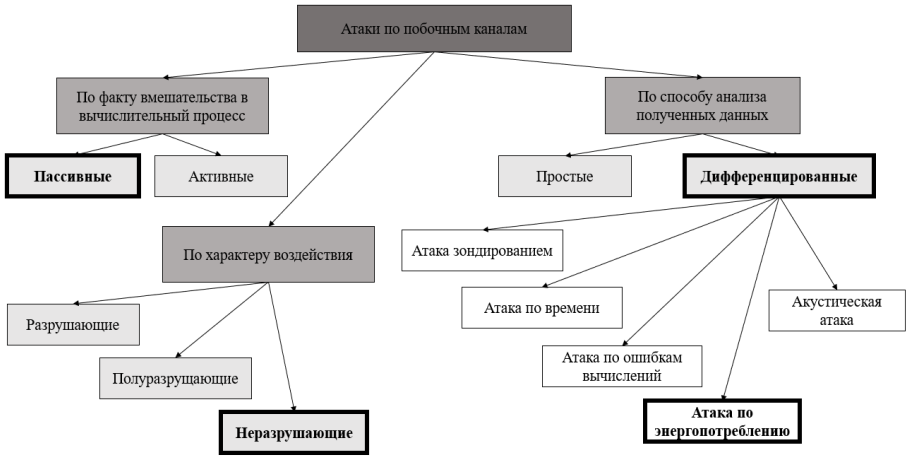

Рис. 1. Классификация атак по побочным каналам.

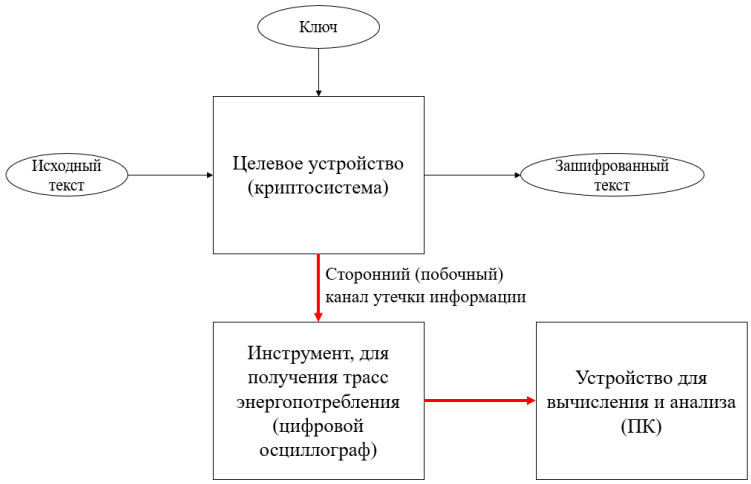

Рис. 2. Структура стенда для проведения атаки по энергопотреблению.

Моделирование энергопотребления с помощью инструмента ELMO. Любое моделирование энергопотребления (или другого побочного канала) состоит из двух составных частей: эмуляция процесса, который выполняется внутри устройства, и моделирование наблюдаемого извне поведения устройства (для сопоставления эмулируемых процессов с прогнозируемым потреблением). Моделирование можно в общих чертах разделить на категории в зависимости от архитектурного уровня, на котором они пытаются охарактеризовать мощность:

1. Моделирование транзисторного уровня. При наличии достаточной информации о технологии, по которой будет построен чип, схему можно сопоставить с сетью транзисторов, потребляемая мощность которых моделируется с помощью известных дифференциальных уравнений.

2. Моделирование уровня шлюза. Данный вид также основан на списках соединений (с обратной аннотацией). Для моделирования количество переходов в каждом шлюзе подсчитывается и взвешивается в соответствии с информацией в списке соединений. Тогда сумма по всем взвешенным переходам является приближением мгновенной мощности схемы.

3. Моделирование поведенческого уровня. На этом уровне нет информации о размещении элементов схемы и маршрутизации сигналов между ними. Доступ имеется только к поведенческому описанию компонентов – например, в форме машинного кода или микрокода низкого уровня, кода инструкции/ассемблера или кода более высокого уровня (например, C). Разработка точных моделей на этом уровне требует доступа к реальным устройствам (и лабораторной установке), с помощью которых оценивается средняя мощность различных (последовательностей) инструкций. Они хорошо подходят для небольших устройств (и, следовательно, низкой сложности), в которых инструкции по сборке сопоставляются непосредственно с машинными инструкциями без дальнейшего декодирования в микроинструкции.

ELMO [17] – это инструмент моделирования, совмещающий несколько категорий из описанных выше. Инструмент ELMO содержит в себе эмулятор конкретной архитектуры (Arm Cortex-M0) с эмпирически оцененными моделями энергопотребления, зависящими от входных данных.

Программное средство ELMO основано на эмуляторе инструкций для Thumb под названием Thumbulator. Thumbulator предназначен для воспроизведения работы процессоров семейства ARM Cortex M0 при выполнении симметричных блочных шифров. Thumbulator принимает на вход двоичную программу на ассемблере Thumb и транслирует ее в машинные инструкции, что позволяет воспроизвести поток данных ядра микропроцессора с достаточной точностью [18].

Для моделирования энергопотребления криптосистем, основанных на ARM Cortex M0, в ELMO интегрированы широко используемые в реализациях симметричной криптографии модели инструкции Thumb. Эти инструкции можно распределить на 5 разных групп:

1) инструкции загрузки (ldr, ldrb, ldrh);
2) инструкции ALU (adds, adds #imm, ands, eors, movs, movs #imm, orrs, subs, subs #imm, cmp, cmp #imm);
3) инструкции сохранения (str, strb, strh);
4) инструкции сдвига (lsls, lsrs, rors);
5) инструкция умножения (muls).

Инструкции с утечкой получены в результате выполнения статистического поиска на основе t-теста в ELMO. Значение параметра t вычисляется по формуле (1):

$$t = \frac{mean_{fix} - mean_{rand}}{\sqrt{\frac{var_{fix}}{N_{fix}} + \frac{var_{rand}}{N_{rand}}}}, \quad (1)$$

где *fix* – группа фиксированных значений,
rand – группа случайных значений,
mean – среднее значение всех трасс в группе,
var – стандартное отклонение выборки всех трасс в группе,
N – размер группы.

Пороговым значением, по которому делается вывод о наличии утечки, зафиксировано значение t = |4.5|, в соответствии с рекомендациями стандарта CSA ISO/IEC 17825-2018 "Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules" [19] по использованию Test Vector Leakage Assessment (TVLA) [20, 21].

Моделирование энергопотребления шифра «Магма». В алгоритме «Магма» для шифрования используется блок размером 64 бита, длина ключа составляет 256 бит. Раундовые ключи получаются из исходного путем его деления на восемь 32-битных подключей (Ki). После получения подключей идет непосредственно процесс шифрования: блок входных данных разделяется на две равные по длине части – правую (R) и левую (L) (по 32 бита каждая), над которыми выполняется тридцать две итерации раундового преобразования с использованием раундовых ключей. На рис. 3 представлена схема раундового преобразования алгоритма «Магма» при шифровании.

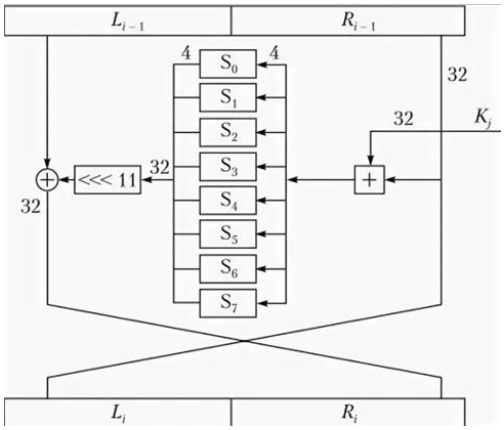

Рис. 3. Схема раундового преобразования алгоритма «Магма»

Проведена оценка общего количества инструкций и количества инструкций, содержащих статистические утечки по энергопотреблению, для различного числа раундов. Результаты моделирования представлены в табл. 1.

На рис. 4 представлена одна трасса энергопотребления полнораундового шифра «Магма». Из данного графика видно, как сначала выполняются служебные инструкции инициализации параметров шифрования (независимые от количества раундов), после чего запускаются группы инструкций раундового преобразования (соответствующие 32 пика).

Таблица 1

Результаты моделирования утечек по побочным каналам для различного количества раундов шифра «Магма»

Кол-во раундов	Общее кол-во инструкций	Инструкции с утечками по энергопотреблению	Процентное соотношение
32	15400	4450	29%
16	8820	2203	25%
2	2992	462	15%
1	2599	277	11%

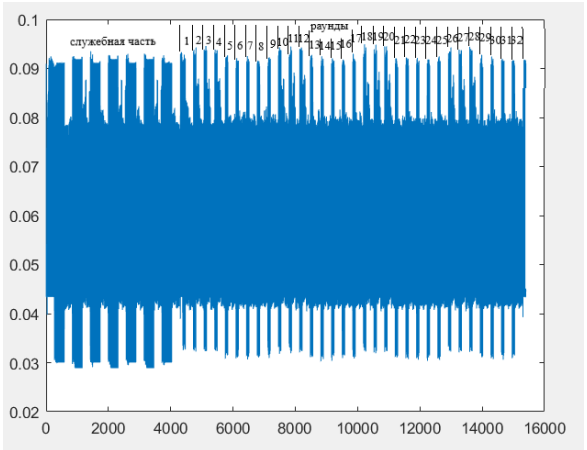

Рис. 4. Сгенерированная с помощью инструмента ELMO трасса энергопотребления при выполнении тридцати двух раундов алгоритма «Магма»

На рис. 5 представлены результаты теста FixedvsRandom для одного раунда шифра «Магма». Наиболее уязвимые для атак посторонним каналам инструкции занесены в табл. 2, курсивом выделены два наибольших значения по результатам статистического теста.

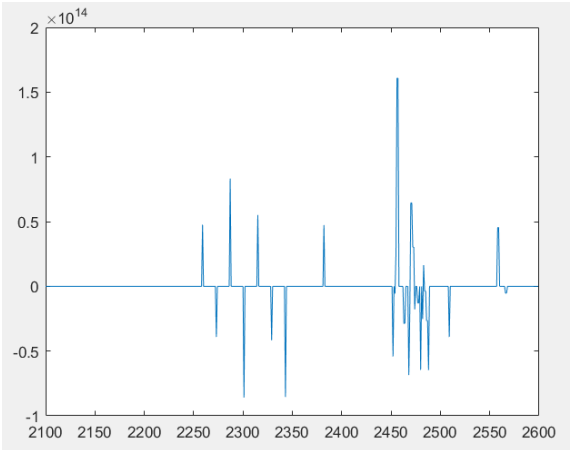

Рис. 5. Результаты применения статистического теста FixedvsRandom в эмуляторе ELMO для одного раунда шифра «Магмы»

Таблица 2

Инструкции, содержащие статистическую зависимость (утечку), для одного раунда шифра «Магма»

Номер инструкции	Адрес	Машинный код	Ассемблерный код инструкции
2287	0x0800014A	0x090B	lsrs r3,r1,#0x4
2301	0x0800014A	0x090B	lsrs r3,r1,#0x4
2343	0x0800014A	0x090B	lsrs r3,r1,#0x4
2456	*0x08000176*	*0x18E3*	*adds r3,r4,r3*
2457	*0x08000178*	*0x5C5B*	*ldrb r3,[r3,r1]*
2468	0x08000172	0x011B	lsls r3,r3,#0x4
2470	0x08000176	0x18E3	adds r3,r4,r3
2471	0x08000178	0x5C5B	ldrb r3,[r3,r1]
2480	0x0800016E	0x090B	lsrs r3,r1,#0x4
2488	0x0800017A	0x5483	strb r3,[r0,r2]

Моделирование энергопотребления шифра «Кузнечик». Шифр «Кузнечик» представляет собой симметричный блочный алгоритм, работающий с блоками данных длинной 128 бит. Размер ключа составляет 256 бит. Основу алгоритма составляет подстановочно-перестановочная сеть (SP-сеть). Алгоритм шифрования «Кузнечик» состоит из выполнения девяти полных раундов, каждый из которых включает в себя три последовательные операции. Первая операция представляет собой сложение по модулю 2 (XOR) ключа и входного блока данных, вторая операция производит нелинейное преобразование, которое представляет собой простую замену одного байта на другой в соответствии с таблицей, третья операция называется линейным преобразованием, при котором каждый байт из блока умножается в поле Галуа на один из коэффициентов ряда (148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194, 16, 133, 32, 148, 1) в зависимости от порядкового номера байта. Затем байты складываются между собой по модулю 2, и весь блок сдвигается в сторону младшего разряда, а полученное число записывается на место считанного байта. Последний десятый раунд является не полным и включает в себя только операцию сложения с ключом.

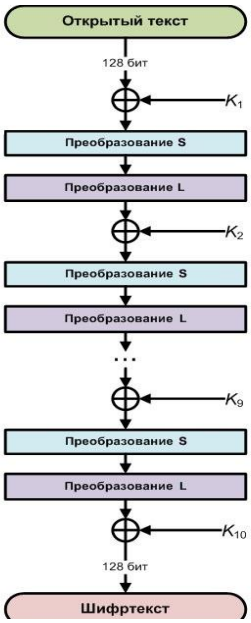

Рис. 6. Схема шифрования алгоритма «Кузнечик»

Аналогично проведенному исследованию утечек по энергопотреблению для шифра «Магма» было вычислено общее количество инструкций для разного количества раундов шифра «Кузнечик» и с помощью статистического t-теста в ELMO выявлены инструкции, содержащие утечку по энергопотреблению. Результаты моделирования трасс энергопотребления шифра «Кузнечик» и исследования инструкций с утечками занесены в табл. 3.

Таблица 3

Результаты моделирования утечек по побочным каналам для различного количества раундов шифра «Кузнечик»

Кол-во раундов	Общее кол-во инструкций	Инструкции с утечками по энергопотреблению	Процентное соотношение
10	7167	4833	67%
5	3735	2492	67%
2	1674	1084	65%
1	970	611	63%

Трасса энергопотребления полнораундового шифра «Кузнечик» показана на рис. 7. На данном графическом представлении визуально выделяются 10 раундов шифрования.

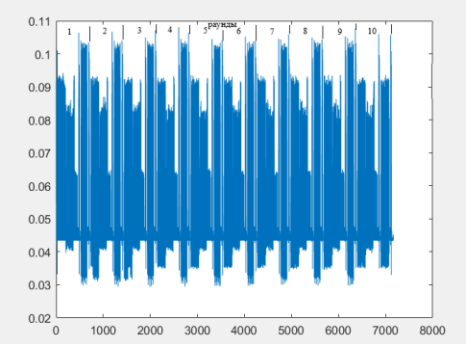

Рис. 7. Сгенерированная с помощью инструмента ELMO трасса энергопотребления при выполнении десяти раундов алгоритма «Кузнечик»

Проведен анализ на базе теста FixedvsRandom для одного раунда шифра «Кузнечик», результаты в графическом виде приведен на рис. 8. В табл. 4 занесены десять инструкций, содержащих выявленные статические утечки по энергопотреблению. Курсивом выделены инструкции, с максимальным отклонением по результатам статистического теста.

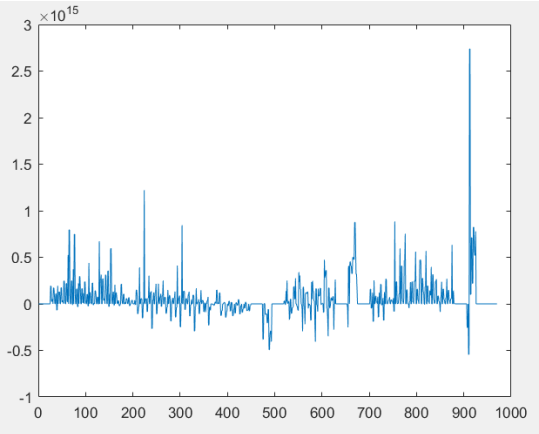

Рис. 8. Результаты применения теста FixedvsRandom в эмуляторе ELMO для одного раунда шифра «Кузнечик»

Таблица 4

Инструкции, содержащие статистическую утечку по энергопотреблению для одного раунда шифра «Кузнечик»

Номер инструкции	Адрес	Машинный код	Ассемблерный код инструкции
65	0x08000192	0x545A	strb r2,[r3,r1]
224	0x080001AA	0x3301	adds r3,#0x01
304	0x080001AA	0x3301	adds r3,#0x01
669	0x080009CA	0x609F str	r7,[r3,#0x20001EA8]
754	0x0800025C	0x702A	strb r2,[r5,#0x20001EA4]
912	*0x080009C0*	*0x001D*	*lsls r5,r3,#0x0*
913	*0x080009C2*	*0x601F*	*str r7,[r3,#0x20000888]*
920	0x080009C8	0x68A7	ldr r7,[r4,#0x20001EA8]
921	0x080009CA	0x609F	str r7,[r3,#0x20000890]
925	0x080009CE	0x3410	adds r4,#0x10

Заключение. В рамках исследования проведено моделирование трасс энергопотребления для различного количества раундов алгоритмов шифрования «Магма» и «Кузнечик». Выделены сигнатуры трасс энергопотребления, соответствующие отдельным раундам и преобразованиям шифрования исследуемого алгоритма. Выполнены наборы статистических тестов (t-тестов), по которым определены инструкции, содержащие утечки для одного раунда шифров «Магма» и «Кузнечик». Сформированные файлы трасс энергопотребления, ассемблерного кода и FxedvsRandom тестов предоставлены в общий доступ для возможности ознакомления и последующего использования результатов моделирования.

Полнораундовая версия алгоритма шифрования «Магма» содержит 15400 инструкций, из них 4450 инструкций содержит потенциальную утечку по энергопотреблению. Для одного раунда шифра «Магма» инструкции с номерами 2456 (adds r3,r4,r3) и 2457 (ldrb r3,[r3,r1]) имеют максимальное значение по статистическому тесту FixedvsRandom.

Полнораундовая версия алгоритма шифрования «Кузнечик» содержит 7167 инструкций, из них 4833 инструкций содержит потенциальную утечку по энергопотреблению. Для одного раунда шифра «Кузнечик» инструкции с номерами 912 (lsls r5,r3,#0x0) и 913 (str r7,[r3,#0x20000888]) имеют максимальное значение по статистическому тесту FixedvsRandom.

Выявленные инструкции и, следовательно, точки на трассах энергопотребления являются оптимальными для проведения анализа стойкости исследуемых реализаций алгоритмов шифрования к атаке по побочному каналу энергопотребления.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Hou X., Breier J.* Side-Channel Analysis Attacks and Countermeasures // Cryptography and Embedded Systems Security. Springer, Cham. – https://doi.org/10.1007/978-3-031-62205-2_4.
2. *Piessens F. and van Oorschot P.C*. Side-Channel Attacks: A Short Tour // IEEE Security & Privacy. – March-April 2024. – Vol. 22, No. 2. – P. 75-80. – DOI: 10.1109/MSEC.2024.3352848.
3. *Kaleem M., Mushtaq M., Ali Ramay S., Aamir Mahmood, Abbas Khan T., Kamran Hussain S., Anwar A., Abdullah Bhatti H.* Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities // Journal of Computing & Biomedical Informatics. – 2024. – 7 (02). – https://jcbi.org/index.php/Main/article/view/626.
4. *Cui X., Zhang H., Xu J., Fang X., Ning W., Wang Y., Hosen M.S.* A Data Augmentation Method for Side-Channel Attacks on Cryptographic Integrated Circuits // Electronics. – 2024. – 13. – 1348. – https://doi.org/10.3390/electronics13071348.
5. *Amrouche A., Boubchir L. and Yahiaoui S.* Side Channel Attack using Machine Learning // 2022 Ninth International Conference on Software Defined Systems (SDS), Paris, France, 2022. – P. 1-5. – DOI: 10.1109/SDS57574.2022.10062906.
6. *Krasovsky A.V. and Maro E.A*. Actual and historical state of side channel attacks theory // Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19). Association for Computing Machinery, New York, NY, USA. – Article 13. – P. 1-7. – https://doi.org/10.1145/3357613.3357627
7. *Kitazawa T., Fujimoto D. and Hayashi Y.* Fundamental Study on Simple Power Analysis Using Backscattering from Switching Regulators // 2024 International Symposium on Electromagnetic Compatibility – EMC Europe, Brugge, Belgium, 2024. – P. 22-26. – DOI: 10.1109/EMCEurope59828.2024.10722404.
8. *Camacho-Ruiz E., Sánchez-Solano S., Martínez-Rodríguez M.C., Tena-Sanchez E. and Brox P.* A Simple Power Analysis of an FPGA implementation of a polynomial multiplier for the NTRU cryptosystem // 2023 38th Conference on Design of Circuits and Integrated Systems (DCIS), Málaga, Spain, 2023. – P. 1-6. – DOI: 10.1109/DCIS58620.2023.10336001.
9. *Xu J., Fan A., Lu M. and Shan W*. Differential Power Analysis of 8-Bit Datapath AES for IoT Applications // 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018. – P. 1470-1473. – DOI: 10.1109/TrustCom/BigDataSE.2018.00205.
10. *Wang W., Yu Y., Standaert F.-X., Liu J., Guo Z. and Gu D*. Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips // IEEE Transactions on Information Forensics and Security. – May 2018. – Vol. 13, No. 5. – P. 1301-1316. – DOI: 10.1109/TIFS.2017.2787985.
11. *Cai X., Li R., Kuang S., Tan J.* An Energy Trace Compression Method for Differential Power Analysis Attack // IEEE Access. – 2020. – Vol. 8. – P. 89084-89092.
12. *Fernandes Medeiros S., Gérard F., Veshchikov N., Lerman L., Markowitch O.* Breaking Kalyna 128/128 with Power Attacks / in Carlet, C., Hasan, M., Saraswat, V. (eds) // Security, Privacy, and Applied Cryptography Engineering. SPACE 2016. Lecture Notes in Computer Science. – Vol. 10076. – Springer, Cham. – https://doi.org/10.1007/978-3-319-49445-6_23.
13. *Jeon Y., Yoon J.W.* Filtering-Based Correlation Power Analysis (CPA) with Signal Envelopes Against Shuffling Methods / You I. (eds) // Information Security Applications. WISA 2020. Lecture Notes in Computer Science. – Vol. 12583. – Springer, Cham. – https://doi.org/10.1007/978-3-030-65299-9_29.
14. *Lo O., Buchanan W.J., Carson D.* Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA) // Journal of Cyber Security Technology. – 2016. – 1 (2). – P. 88-107. – https://doi.org/10.1080/23742917.2016.1231523.
15. *Xin J., Du Z.* Template attack based on uBlock cipher algorithm // Frontiers in Computing and Intelligent Systems. – 2023. – 3 (1). – P. 90-93. – https://doi.org/10.54097/fcis.v3i1.6031.
16. ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры. – URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
17. Statistical leakage simulator for the ARM M0 family ELMO. – URL: https://github.com/scaresearch/ELMO.

18. *Welch D.* Thumbulator. – URL: https://github.com/dwelch67/thumbulator.git.
19. CSA ISO/IEC 17825-2018 Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules.
20. *Goodwill G., Jun B., Jaffe J. and Rohatgi P*. A testing methodology for side-channel resistance validation // NIST Non-Invasive At-tack Testing Workshop. – 2011.
21. *Cooper J., DeMulder E., Goodwill G., Jaffe J., Kenworthy G. and Rohatgi P.* Test vector leakage assessment (tvla) methodology in practice // International Cryptographic Module Conference. – 2013.

REFERENCES

1. *Hou X., Breier J.* Side-Channel Analysis Attacks and Countermeasures, *Cryptography and Embedded Systems Security. Springer, Cham*. Available at: https://doi.org/10.1007/978-3-031-62205-2_4.
2. *Piessens F. and van Oorschot P.C*. Side-Channel Attacks: A Short Tour, *IEEE Security & Privacy,* March-April 2024, Vol. 22, No. 2, pp. 75-80. DOI: 10.1109/MSEC.2024.3352848.
3. *Kaleem M., Mushtaq M., Ali Ramay S., Aamir Mahmood, Abbas Khan T., Kamran Hussain S., Anwar A., Abdullah Bhatti H.* Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities, *Journal of Computing & Biomedical Informatics,* 2024, 7 (02). Available at: https://jcbi.org/index.php/Main/article/view/626.
4. *Cui X., Zhang H., Xu J., Fang X., Ning W., Wang Y., Hosen M.S.* A Data Augmentation Method for Side-Channel Attacks on Cryptographic Integrated Circuits, *Electronics,* 2024, 13, 1348. Available at: https://doi.org/10.3390/electronics13071348.
5. *Amrouche A., Boubchir L. and Yahiaoui S.* Side Channel Attack using Machine Learning, *2022 Ninth International Conference on Software Defined Systems (SDS), Paris, France, 2022,* pp. 1-5. DOI: 10.1109/SDS57574.2022.10062906.
6. *Krasovsky A.V. and Maro E.A*. Actual and historical state of side channel attacks theory, *Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19). Association for Computing Machinery, New York, NY, USA,* Article 13, pp. 1-7. Available at: https://doi.org/10.1145/3357613.3357627
7. *Kitazawa T., Fujimoto D. and Hayashi Y.* Fundamental Study on Simple Power Analysis Using Backscattering from Switching Regulators, *2024 International Symposium on Electromagnetic Compatibility – EMC Europe, Brugge, Belgium, 2024,* pp. 22-26. DOI: 10.1109/EMCEurope59828.2024.10722404.
8. *Camacho-Ruiz E., Sánchez-Solano S., Martínez-Rodríguez M.C., Tena-Sanchez E. and Brox P.* A Simple Power Analysis of an FPGA implementation of a polynomial multiplier for the NTRU cryptosystem, *2023 38th Conference on Design of Circuits and Integrated Systems (DCIS), Málaga, Spain, 2023,* pp. 1-6. DOI: 10.1109/DCIS58620.2023.10336001.
9. *Xu J., Fan A., Lu M. and Shan W*. Differential Power Analysis of 8-Bit Datapath AES for IoT Applications, *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018,* pp. 1470-1473. DOI: 10.1109/TrustCom/BigDataSE.2018.00205.
10. *Wang W., Yu Y., Standaert F.-X., Liu J., Guo Z. and Gu D*. Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips, *IEEE Transactions on Information Forensics and Security,* May 2018, Vol. 13, No. 5, pp. 1301-1316. DOI: 10.1109/TIFS.2017.2787985.
11. *Cai X., Li R., Kuang S., Tan J.* An Energy Trace Compression Method for Differential Power Analysis Attack, *IEEE Access,* 2020, Vol. 8, pp. 89084-89092.
12. *Fernandes Medeiros S., Gérard F., Veshchikov N., Lerman L., Markowitch O.* Breaking Kalyna 128/128 with Power Attacks, in Carlet, C., Hasan, M., Saraswat, V. (eds), *Security, Privacy, and Applied Cryptography Engineering. SPACE 2016. Lecture Notes in Computer Science,* Vol. 10076. Springer, Cham. Available at: https://doi.org/10.1007/978-3-319-49445-6_23.
13. *Jeon Y., Yoon J.W.* Filtering-Based Correlation Power Analysis (CPA) with Signal Envelopes Against Shuffling Methods, You, I. (eds), *Information Security Applications. WISA 2020. Lecture Notes in Computer Science,* Vol. 12583. Springer, Cham. Available at: https://doi.org/10.1007/978-3-030-65299-9_29.
14. *Lo O., Buchanan W.J., Carson D.* Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA), *Journal of Cyber Security Technology,* 2016, 1 (2), pp. 88-107. Available at: https://doi.org/10.1080/23742917.2016.1231523.
15. *Xin J., Du Z.* Template attack based on uBlock cipher algorithm, *Frontiers in Computing and Intelligent Systems,* 2023, 3 (1), pp. 90-93. Available at: https://doi.org/10.54097/fcis.v3i1.6031.
16. GOST R 34.12-2015 Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry [GOST R 34.12-2015 Information technology. Cryptographic protection of information. Block ciphers]. Available at: URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf.

17. Statistical leakage simulator for the ARM M0 family ELMO. Available at:https://github.com/scaresearch/ELMO.
18. *Welch D*. Thumbulator. Available at: https://github.com/dwelch67/thumbulator.git.
19. CSA ISO/IEC 17825-2018 Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules.
20. *Goodwill G., Jun B., Jaffe J. and Rohatgi P*. A testing methodology for side-channel resistance validation, *NIST Non-Invasive At-tack Testing Workshop,* 2011.
21. *Cooper J., DeMulder E., Goodwill G., Jaffe J., Kenworthy G. and Rohatgi P.* Test vector leakage assessment (tvla) methodology in practice, *International Cryptographic Module Conference,* 2013.

Статью рекомендовал к опубликованию д.т.н., профессор А.Н. Целых.

Малявина Виктория Олеговна – Южный федеральный университет; e-mail: malyavina@sfedu.ru; г. Таганрог, Россия; тел.: 88634371905; кафедра безопасности информационных технологий им. О.Б. Макаревича; выпускник.

Маро Екатерина Александровна – e-mail: eamaro@sfedu.ru; тел.: 88634371905; кафедра безопасности информационных технологий им. О.Б. Макаревича; к.т.н.; доцент.

Malyavina Viktoriya Olegovna – Southern Federal University; e-mail: malyavina@sfedu.ru; Taganrog, Russia; phone: +78634371905; the Department of Information Security; alumnus.

Maro Ekaterina Aleksandrovna – e-mail: eamaro@sfedu.ru; phone: +78634371905; the Department of Information Security; cand. of eng. sc.; associate professor.

УДК 004.272.44 DOI 10.18522/2311-3103-2024-5-173-185

Д.А. Сорокин, А.В. Касаркин

ОБЗОР МОДЕЛЕЙ КОММУТАЦИОННЫХ ПОДСИСТЕМ ЦИФРОВЫХ ФОТОННЫХ ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ

Рассматриваются варианты организации подсистемы коммутации цифровых фотонных вычислительных устройств, основной задачей которой является обеспечение возможности организации эффективных вычислений при решении задач различных проблемных областей. По мнению авторов, цифровые фотонные вычислители должны обрабатывать информацию в структурной парадигме вычислений. Данная парадигма принципиально отличается от классической фон-Неймановской парадигмы, поскольку в ней передача данных между функциональными элементами не расторжима с обработкой. Поэтому проблематика построения подсистемы коммутации в разрабатываемых цифровых фотонных вычислительных устройствах – одна из ключевых. Данная подсистема должна обрабатывать информационные зависимости между выполняемыми операциями не только во времени, но и в пространстве. Только в этом случае обработка данных в фотонных вычислительных системах будет выполняться с производительностью, превосходящей на два и более десятичных порядка производительность самых современных электронных вычислительных систем. Рассматриваются вопросы обеспечения потокового обмена данными между функциональными устройствами в цифровом фотонном вычислителе. Авторы разработали и проанализировали в базисе фотонной логики модели коммутационных устройств и способы организации коммутационной подсистемы при выполнении последовательной обработки данных. В ходе исследований было установлено, что структурная организация вычислений в цифровых фотонных вычислителях возможна при обеспечении обмена данными посредством пространственной коммутации входных и выходных каналов функциональных устройств. При реализации цифровых фотонных вычислителей как универсальных устройств, ориентированных на широкий класс задач, наиболее удобными для организации вычислительных структур будут иерархический и иерархическо-кольцевой варианты подсистемы коммутации. Однако данные варианты характеризуются высокими накладными расходами на построение коммутаторов. Поэтому в проблемно-ориентированных фотонных вычислителях, предназначенных для решения сильносвязанных задач с высокой удельной производительностью, более предпочтительно применение ортогональной или тороидальной подсистемы коммутации. В этом случае должна обеспечиваться непосредственная пространственная коммутация между функциональными устройствами одной группы,