УДК 004.056.5 doi: 10.26102/2310-6018/2018.23.4.034

В.А. Минаев, Е. В. Зеленцова, С. С. Петров

АТАКИ ПО ВРЕМЕНИ НА ИНФОРМАЦИЮ В НЕДОВЕРЕННЫХ СРЕДАХ

ФГБОУ ВО «Московский государственный технический университет» им. Н.Э. Баумана МГТУ (национальный исследовательский университет)

Актуальность совершенствования программно-алгоритмической защиты аппаратных устройств, работающих в недоверенных средах (НС), обусловлена тем, что они с наибольшей вероятностью подвержены воздействию с целью нарушения функционирования их внутренней структуры. Цель статьи – анализ, оценка эффективности, прогнозирование развития перспективных средств и методов атак на информацию в НС. В статье приведен детальный анализ характеристик таких атак. Уделено внимание алгоритмическим и аппаратным методам защиты информации от атак по времени. Среди таких атак рассмотрены использующие кэш-память, анализ энергопотребления и характеристик электромагнитных полей. Результаты и выводы следующие. Показаны преимущества атак по времени перед другими методами атак по побочным каналам: не требуется дорогостоящее лабораторное оборудование; могут быть реализованы удаленно, без физического доступа к атакуемому средству защиты информации; могут быть включены как часть комплексной атаки. Недостатками атак по времени являются: необходимость высокой точности определения времени выполнения операции шифрования; требование большого объема данных для анализа; понимание всех особенностей реализации используемого алгоритма, используемого при этом типа процессора, его архитектуры; наличие доступа к кэш-памяти, которую использует исследуемый процесс. Недостатки методов противодействия атакам по времени: они не являются комплексными; могут создавать побочный канал утечки информации; отсутствуют оценки их эффективности. Полученные результаты представляют ценность при практической организации защиты информации в НС.

Ключевые слова: защита информации, недоверенная среда, атака по времени, анализ энергопотребления, электромагнитное поле, алгоритмические и аппаратные методы

ВВЕДЕНИЕ

С развитием программных средств и уменьшением стоимости специального оборудования возрастает актуальность программно-алгоритмической защиты аппаратных устройств, работающих в недоверенных средах (НС). Такие устройства, работающие в НС, как правило, с наибольшей вероятностью подвержены внешнему воздействию с целью нарушения функционирования их внутренней структуры. Ключевая информация может быть извлечена с помощью методов анализа аппаратных реализаций и эффективно использована злоумышленником в негативных направлениях.

Необходимо подчеркнуть, что в целях взлома теоретически весьма стойкого алгоритма защиты информации злоумышленник, в первую очередь, анализирует практическую реализацию алгоритма, а не его математическую модель, весьма строгую и логичную.

Независимо от устройства, на котором реализован алгоритм, его выполнение обязательно оставляет свой след в самом устройстве или в окружающих его и связанных с ним объектах и пространстве. Этот след может содержать информационные следы о внутреннем состоянии средства защиты информации, которая недоступна при классическом крипто анализе.

Убедительные математические обоснования, которые гарантируют стойкость алгоритма, обычно не играют главенствующей роли при наличии таких информационных следов, носящих, вообще говоря, косвенный характер.

Например, при выполнении алгоритма шифрования на каком-либо процессоре, последний оставляет след в виде потребляемой им энергии. Этот след может содержать информацию об обрабатываемых процессором данных, что может быть использовано злоумышленниками для получения за короткий промежуток времени информации о секретном ключе. Такие каналы утечки информации выступают в качестве побочных, а атаки, их использующие, называются атаками по побочным каналам. В связи с этим все более актуальными становятся задачами обеспечения безопасности реализаций алгоритмов защиты информации от анализа в НС, используемых в информационных системах различного уровня и назначения.

Проблемой обеспечения безопасности алгоритмов защиты информации от анализа в НС в последние годы занимались многие ученые: С. П. Панасенко [1], С.П. Скоробогатов [2], P. Kocher [3], F. Standaert [4], W. Schindler [5], A. Shamir [6]. Однако и до сих пор данная проблема далека от окончательного решения, поскольку предлагаемые методы защиты либо недостаточно универсальны и эффективны, либо слабо формализованы.

МАТЕРИАЛ И МЕТОДЫ

Рассмотрим основные характеристики атак на информацию в недоверенных средах.

Агрессивные атаки требуют разборки устройства для непосредственного доступа к его компонентам, например подключение к шине данных для перехвата данных.

Неагрессивные атаки используют только информацию, доступную извне, например, время выполнения операций, данные о потреблении энергии, электромагнитном излучении.

Агрессивные атаки требуют дорогостоящего лабораторного оборудования, поэтому встречаются достаточно редко и направлены на конкретные устройства.

Для реализации *активных атак* необходимо вмешательство в функционирование системы, например, атака по ошибкам вычислений требует воздействия на устройство с целью возникновения искажения информации в процессе обработки. *Пассивные атаки* отражают невмешательство в процесс функционирования устройства, характеризуясь наблюдением за его поведением в процессе работы.

Простые атаки представляют собой исследование прямой зависимости между операциями, осуществляемыми устройством и полученной злоумышленником информацией, при этом сигнал полезной информации из побочного канала утечки должен быть отделен от шумов.

В *дифференциальных атаках* для исследования зависимости между входными данными и информацией из побочного канала используются статистические методы, реализуемые на основе специально создаваемой теоретической модели функционирования устройства.

В настоящей статье из всего спектра реализаций алгоритмов защиты информации в НС на основе анализа зарубежных источников рассмотрены только те, которые перспективны для использования в недоверенных средах и отличаются:

1. Повышенной сложностью получения необходимых данных об объекте информационной защиты путём добавления случайных задержек, добавления фиктивных инструкций, введения случайного порядка выполнения операций.
2. Заменой критических инструкций такими, которые сложно анализировать; уникальным перестроением критических алгоритмов арифметических операций или работы памяти.
3. Внесение алгоритмических изменений в криптографические примитивы таким образом, чтобы атаки были мало эффективны, например, путем шифрования данных и ключа случайными масками.

В работах [7, 8] показано, что данные подходы к защите и универсальны, и достаточно эффективны при правильной реализации.

Программно-ориентированные методы защиты включают в себя добавление случайных инструкций, случайный порядок выполнения инструкций и др. Программные методы противодействия атакам по побочным каналам значительно затрудняют работу алгоритмов, критически

увеличивая количество используемой памяти и уменьшая производительность.

На аппаратном же уровне методы защиты обычно включают в себя случайные задержки, случайное или сглаженное потребление энергии, случайный порядок выполнения инструкций или использования регистров.

В большинстве случаев сочетание аппаратных и программных методов противодействия дает наилучшее соотношение безопасности и стоимости защиты.

Алгоритмические методы защиты

Случайные последовательности. Самый распространенный метод противодействия атакам – имитировать случайный характер информации в побочных каналах утечки. Недостаток метода заключается в том, что сложно гарантировать, что злоумышленник не может получить какие-либо полезные данные о начальном состоянии и/или промежуточных данных во время вычислений, чтобы исключить возможность статистического анализа.

Разделение вычислительного процесса не позволяет клиенту вычислить некоторую математическую функцию из-за наличия у провайдера секретных параметров, необходимых для её вычисления. Впервые такая технология применена для алгоритма RSA, являясь одной из наиболее эффективных против удаленного анализа по времени выполнения, а также против анализа энергопотребления и/или временного анализа аппаратных средств защиты информации.

Маскировка обрабатываемых данных – наиболее распространенный метод противодействия атакам по времени выполнения и атакам по энергопотреблению, предполагающий использование масок для сокрытия промежуточных значений, обрабатываемых в процессе работы алгоритма защиты информации. Первая схема маскировки предложена в [8] для алгоритма DES. Изначально большинство из этих схем являлись маскировками первого порядка, разделяющими каждую переменную на две составляющие – маску и замаскированные данные. Затем были разработаны схемы маскировки более высокого порядка, позволяющие противодействовать атакам, использующим утечку промежуточных результатов вычислений.

Аппаратные методы защиты

После публикации Кохера [4], показавшего возможность использования побочных каналов утечки для анализа криптографических устройств, атаки по побочным каналам стали наиболее значимой угрозой безопасности. Данные атаки основываются на анализе утечек информации

в результате изменения энергопотребления, электромагнитного излучения устройства и учете времени обработки данных.

С тех пор, как данные уязвимости обнаружены, предложено множество методов противодействия соответствующим атакам. Эти решения, как правило, направлены на уменьшение зависимости физических свойств устройств от данных, которые они обрабатывают. Эта задача решается путем выравнивания или добавления случайных последовательностей в информацию побочных каналов.

Был разработан метод Dual-Rail-Recharging (DRP) [9], на основе которого созданы процедуры Sense Amplifier Based Logic (SABL) [10] и Wave Dynamic Differential Logic (WDDL) [11]. Еще одним методом является маскировка, наиболее известные его реализации – Random Switching Logic (RSL) [12] и Dual Random Switching Logic (RDSL) [13], основанные на маскировке всех промежуточных значений.

Говоря о модели нарушителя, предполагается, что он является пользователем, имеющим физический доступ к устройству, и способен:

- подбирать входные данные и перехватывать выходные данные средства защиты информации;
- обладает знаниями об используемых алгоритмах защиты информации и особенностях их реализаций;
- использовать все возможные средства анализа, позволяющие получать сведения о работе устройства;
- вносить ошибки в работу средства защиты информации путем физического воздействия на устройство.

Для обеспечения безопасности аппаратных реализаций алгоритмов защиты информации в соответствии с представленной моделью нарушителя в работе решается задача разработки технических решений, направленных на исключение возможности проведения атаки.

Возможность проведения атаки определяется согласно результатам статистических исследований. Для обеспечения безопасности информации предлагается:

1. Исследовать используемые в реализациях операции на возможность использования их в качестве побочного канала утечки информации.
2. Разработать методику увеличения неопределенности данных, получаемых из побочного канала утечки, используя алгоритмические методы и аппаратные особенности вычислительного устройства.
3. Разработать методы защиты от использования аппаратных особенностей в целях проведения атаки по времени выполнения.
4. Разработать методику оценки надежности предложенных методов обеспечения безопасности реализации алгоритма.

ОБСУЖДЕНИЕ

Время выполнения операций по обработке информации является переменной, исследуя которую злоумышленник может определить секретные параметры. Данный класс атак называется атакой по времени выполнения (timing attacks), впервые описанной Кохером [4] и затем примененной на практике против алгоритма RSA, реализованного с использованием алгоритма Монтгомери [14].

Атака по времени была значительно улучшена в работах [15, 16] и с ее помощью удалось восстановить ключ длиной 512 бит, используя от 5000 до 10000 измерений во времени.

В работе [17] представлена атака, использующую китайскую теорему об остатках. Данная атака оказалась достаточно результативной и позволила восстановить 1024 бита ключа при 370 измерениях.

Блочные шифры также являются целью данной атаки. В [16] представлена реализация атаки на алгоритм AES, которая позволила восстановить ключ при помощи 4000 измерений.

Разновидностью атак по времени является Time-Driven Cache Attack, использующая особенности использования злоумышленником сверхоперативной памяти (кэш-памяти) для определения внутреннего состояния устройства или секретного ключа.

Для получения информации о ключах он может использовать побочные косвенные данные, например, измерять потребление энергии во время выполнения функции подстановки. На Рисунке 1 представлен пример графика энергопотребления устройства при попадании в кэш, на Рисунке 2 – при промахе [18].

По представленным на Рисунках 1 и 2 графикам видно, что при промахе резко возрастает энергопотребление устройства шифрования, что дает достаточно информации о выполняемых операциях и позволяет делать косвенные выводы о выполняемых операциях для восстановления секретного ключа.

Данный вид атак применим практически к любому алгоритму защиты информации, реализованному с использованием кэш-памяти. Он применен к наиболее известным алгоритмам защиты информации, используется в средах виртуальных машин и может быть реализован без физического взаимодействия со средством защиты информации.

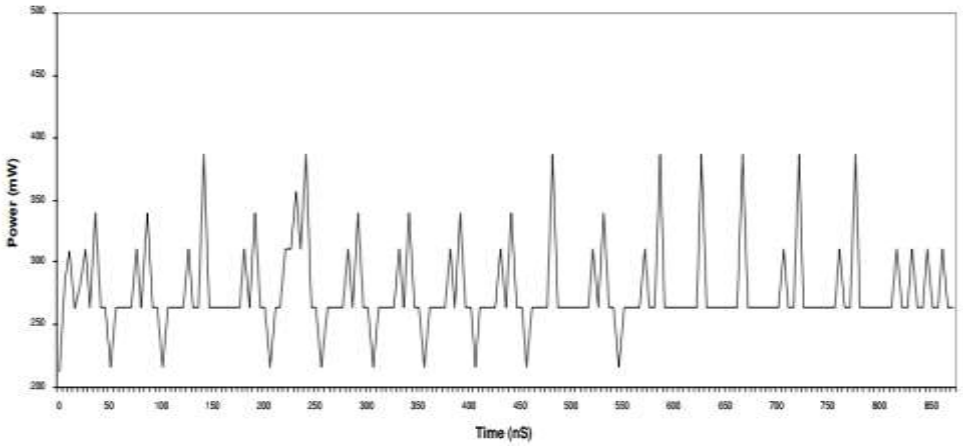

Рисунок 1 – Энергопотребление устройства при попадании в кэш

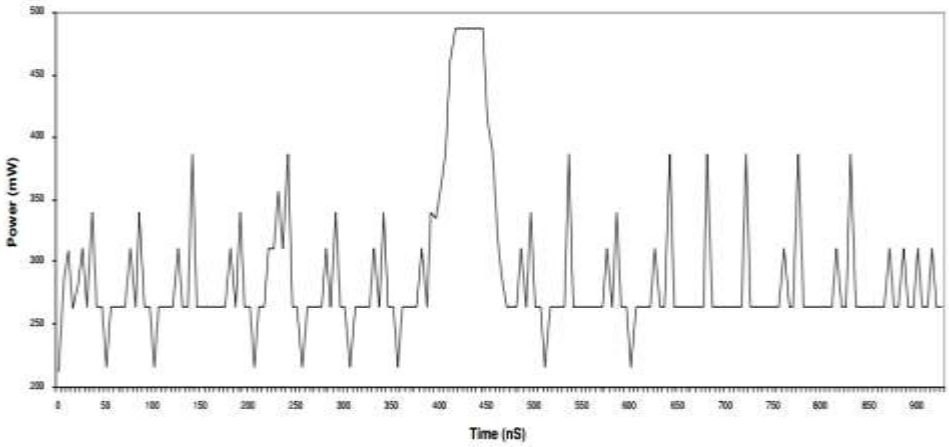

Рисунок 2 – Энергопотребление устройства при промахе кэша

Метод анализа энергопотребления предполагает его прямую зависимость от выполняемых криптографических операций. В алгоритме DES данный тип атаки может быть применен к операциям, использующим:

- *условные операторы*, которые могут вызывать значительные изменения в энергопотреблении устройства, в зависимости от их входа;
- *операции умножения*, которые являются источником утечки данных, которых они обрабатывают.

Кроме изменения энергопотребления в зависимости от выполняемого набора инструкций также существуют эффекты, которые можно соотнести с обрабатываемыми данными. Они менее выражены и иногда могут быть

потеряны в результате ошибок измерения или шумов. Для обнаружения этих эффектов используются статистические функции.

После опубликования алгоритма атаки по анализу энергопотребления появилось большое количество работ, посвященных данной тематике. Появилось важное улучшение метода, связанное с возникновением атаки по энергопотреблению высокого порядка [19].

Аналогичным образом может быть проанализирована информация об электромагнитных полях устройств [20, 21], содержащих подчас больше информации об устройствах и обрабатываемых в них данных, чем информация об энергопотреблении. Согласно [22] возможно составление библиотеки соотношений между инструкциями и их электромагнитным излучением путем использования статистических методов и нейронных сетей.

Несмотря на то, что атаки с использованием электромагнитных полей не являются агрессивными, они более эффективны, обеспечивая более точные измерения.

ЗАКЛЮЧЕНИЕ

1. Атаки по времени, применяемые как в программных, так и аппаратных реализациях имеют ряд преимуществ перед другими методами атак по побочным каналам: для их проведения не требуется дорогостоящее лабораторное оборудование; они могут быть реализованы удаленно, без физического доступа к атакуемому средству защиты информации, используясь на облачных серверах и в виртуализированных средах; могут быть частью комплексной атаки, объединяющей в себе несколько методов анализа информации по побочным каналам.

2. Среди недостатков атак по времени можно выделить: необходимость высокой точности определения времени выполнения операции шифрования; требуется большой объем данных, измеренных на одном ключе шифрования для проведения статистического анализа; нужно знать все особенности реализации используемого алгоритма; в случае работы с кэш-памятью необходимо иметь информацию об используемом типе процессора, его архитектуре, иметь доступ к кэш-памяти, которую использует исследуемый процесс.

3. При рассмотрении существующих методов противодействия атакам по времени выявлены следующие их недостатки: они не являются комплексными и защищают только от одной конкретной атаки, при этом сами могут создавать побочный канал утечки информации; отсутствуют качественные и количественные оценки эффективности данных методов.

ЛИТЕРАТУРА

1. Панасенко, С. П. Атаки на шифраторы, использующие утечки данных по побочным каналам. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. – 576 с.
2. Skorobogatov, S. P. Side-Channel Attacks: New Directions and Horizons // Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) (3 June 2011). Albena. Bulgaria.
3. Kocher, P. Timing Attacks on Implementations of Diffie-Hellmann, RSA, DSS, and Other Systems // Advances in Cryptology — CRYPTO '96. Lecture Notes in Computer Science. 1996. Vol. 1109. — Pp. 104 - 113.
4. Poussier, R., Standaert, F., Grosso, V. Simple Key Enumeration (and Rank Estimation) Using Histograms: An Integrated Approach // CHES. 2016. Pp. 61–81.
5. Schindler, W., Lemke, K., Paar, C. A Stochastic Model for Differential Side Channel Cryptanalysis // CHES. 2005. Pp. 30–46.
6. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems // CRYPTO'90 & Journal of Cryptology. 1991. Vol. 4, Issue 1. – Pp. 3 - 72.
7. Chari, S., Jutla, C., Rao, J., Rohatgi, P. Towards Sound Approaches to Counteract Power-Analysis Attacks. Crypto'99. Springer-Verlag. – Pp. 398 – 411.
8. Goubin, L., Patarin, J. DES and Differential Power Analysis. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-48059-5_15.pdf.
9. Shivani, M., Padmini, C. Enhanced Delay-based Dual-rail Precharge Logic against Leakage Power Analysis Attack // International Journal of Current Engineering and Technology. 2015. Vol. 5, No. 4. – Pp. 2800-2803.
10. Tiri, K., Verbauwhede, I. Charge Recycling Sense Amplifier Based Logic: Securing Low Power Security IC’s against Differential Power Analysis. URL: https://eprint.iacr.org/2004/067.pdf .
11. Tiri, K., Hwang, D., Hodj, A., Lai Bo-Cheng, Yang, S., Schaumont, P., Verbauwhede, I. Prototype IC with WDDL and Differential Routing – DPA ResistanceAssessment. URL: https://www.iacr.org/archive/ches2005/026.pdf .
12. Mizuno, H., Iwai, K., Tanaka, H., Kurokawa, T. A Correlation Power Analysis Countermeasure for Enocoro-128 v2 Using Random Switching Logic.URL:https://www.computer.org/csdl/proceedings/icnc/2012/4893/00/4893 a326. pdf .
13. Chen, Z., Zhou, Y. Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage. URL:

http://www.sciweavers.org/read/dual-rail-random-switching-logic-a-countermeasure-to-reduce-side-channel-leakage-187407

14. Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestr, P., Quisquater, J.-J., Willems, J.-L. A Practical Implementation of the Timing Attack. Technical Report CG1998/1. Brussels: Universities catholique de Louvain, 1998. – 19 p.
15. Schindler, W. Optimized timing attacks against public key cryptosystems // Statistics & Decisions. 2002. No 20 (2). – Pp.191-210.
16. Schindler, W., Koeune, F., Quisquater, J.-J. Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection/Correction Strategies // Proc. of 8th IMA International Conference on Cryptography and Coding. 2001. – Pp. 245 - 267.
17. Schindler, W. A Timing Attack against RSA with the Chinese Remainder Theorem. URL: https://tls.mbed.org/public/WSchindler-RSA_Timing_Attack.pdf
18. Bertoni, G., Zaccaria, V., Breveglieri, L., Monchiero, M., Palermo, G. AES Power Attack Based on Induced Cache Miss and Countermeasure / IEEE Computer Society, 2005. Information Technology: Coding and Computing, International Conference. Apr. 4. 2005. Las Vegas, Nevada. – Pp. 586-591.
19. Messerges, T. Using Second-Order Power Analysis to Attack DPA Resistant Software. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-44499-8_19.pdf .
20. Quisquater, J.-J., Samyde, D. Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. Smart Cards Programming and Security (e-Smart 2001). Lectures Notes in Computer Science (LNCS). 2001. Vol. 2140. Springer. – Pp. 200—210.
21. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P. The EM Side Channel(s): Attacks and Assessment Methodologies. In Cryptographic Hardware and Embedded Systems // CHES 2002, LNCS 2523. Springer-Verlag. – Pp. 29–45.
22. Quisquater, J.-J., Samyde, D. Automatic Code Recognition for Smart Cards Using a Kohonen Neural Network. URL: https://www.usenix.org/legacy /event/cardis02/full papers/quisquater/quisquater.pdf.

V. A. Minaev, E. V. Zelentsova, S. S. Petrov

TIMING ATTACKS ON INFORMATION IN UNTRUSTED ENVIRONMENTS

Bauman Moscow State Technical University

The relevance of improving the software and algorithmic protection of hardware devices operating in untrusted environments (UTE), due to the fact that they are most likely to be exposed to the purpose of disruption of their internal structure. The purpose of the article is to analyze, evaluate the effectiveness, and predict the development of promising tools and methods of attacks on information in the UTE. The article discusses the main characteristics of attacks on information in untrusted environments. A detailed analysis of these characteristics is given. Attention is paid to algorithmic and hardware methods of information protection from time attacks. Among these attacks are considered using cache memory, analysis of power consumption and characteristics of electromagnetic fields. The advantages of attacks over other methods of side-channel attacks are shown: no expensive laboratory equipment is required; they can be implemented remotely, without physical access to the attacked information security tool; can be included as part of a complex attack. The disadvantages of time attacks are: the need for high accuracy of determining the time of the encryption operation; the requirement of a large amount of data for analysis; understanding of all the features of the implementation of the algorithm used in this type of processor, its architecture; the availability of access to the cache memory used by the process under study. Among the shortcomings of the methods of countering attacks over time are: they are not complex; they can create a side channel of information leakage; there are no estimates of their effectiveness. The results are valuable in the practical organization of information protection in UTE.

Keywords: information protection, untrusted environment, time attack, energy consumption analysis, electromagnetic field, algorithmic and hardware methods

REFERENCES

1. Panasenko, S. P. Ataki na shifratory, ispol'zuyushchie utechki dannyh po pobochnym kanalam. Algoritmy shifrovaniya. Special'nyj spravochnik. SPb.: BHV-Petersburg, 2009. – 576 p.
2. Skorobogatov, S. P. Side-Channel Attacks: New Directions and Horizons // Design and Security of Cryptographic Algorithms and Devices (ECRYPT II) (3 June 2011). Albena. Bulgaria.
3. Kocher, P. Timing Attacks on Implementations of Diffie-Hellmann, RSA, DSS, and Other Systems // Advances in Cryptology — CRYPTO '96. Lecture Notes in Computer Science. 1996. Vol. 1109. — Pp. 104 - 113.
4. Poussier, R., Standaert, F., Grosso, V. Simple Key Enumeration (and Rank Estimation) Using Histograms: An Integrated Approach // CHES. 2016. Pp. 61–81.

5. Schindler, W., Lemke, K., Paar, C. A Stochastic Model for Differential Side Channel Cryptanalysis // CHES. 2005. Pp. 30–46.
6. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems // CRYPTO'90 & Journal of Cryptology. 1991. Vol. 4, Issue 1. – Pp. 3 - 72.
7. Chari, S., Jutla, C., Rao, J., Rohatgi, P. Towards Sound Approaches to Counteract Power-Analysis Attacks. Crypto'99. Springer-Verlag. – Pp. 398 – 411.
8. Goubin, L., Patarin, J. DES and Differential Power Analysis. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-48059-5_15.pdf.
9. Shivani, M., Padmini, C. Enhanced Delay-based Dual-rail Precharge Logic against Leakage Power Analysis Attack // International Journal of Current Engineering and Technology. 2015. Vol. 5, No. 4. – Pp. 2800-2803.
10. Tiri, K., Verbauwhede, I. Charge Recycling Sense Amplifier Based Logic: Securing Low Power Security IC's against Differential Power Analysis. URL: https://eprint.iacr.org/2004/067.pdf .
11. Tiri, K., Hwang, D., Hodj, A., Lai Bo-Cheng, Yang, S., Schaumont, P., Verbauwhede, I. Prototype IC with WDDL and Differential Routing – DPA ResistanceAssessment. URL: https://www.iacr.org/archive/ches2005/026.pdf .
12. Mizuno, H., Iwai, K., Tanaka, H., Kurokawa, T. A Correlation Power Analysis Countermeasure for Enocoro-128 v2 Using Random Switching Logic. URL: https://www.computer.org/csdl/proceedings/icnc/2012/4893/00/4893 a326. pdf .
13. Chen, Z., Zhou, Y. Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage. URL: http://www.sciweavers.org/read/dual-rail-random-switching-logic-a-countermeasure-to-reduce-side-channel-leakage-187407
14. Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestr, P., Quisquater, J.-J., Willems, J.-L. A Practical Implementation of the Timing Attack. Technical Report CG1998/1. Brussels: Universities catholique de Louvain, 1998. – 19 p.
15. Schindler, W. Optimized timing attacks against public key cryptosystems // Statistics & Decisions. 2002. No 20 (2). – Pp.191-210.
16. Schindler, W., Koeune, F., Quisquater, J.-J. Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection/Correction Strategies // Proc. of 8th IMA International Conference on Cryptography and Coding. 2001. – Pp. 245 - 267.
17. Schindler, W. A Timing Attack against RSA with the Chinese Remainder Theorem. URL: https://tls.mbed.org/public/WSchindler-RSA_Timing_Attack.pdf
18. Bertoni, G., Zaccaria, V., Breveglieri, L., Monchiero, M., Palermo, G. AES Power Attack Based on Induced Cache Miss and Countermeasure / IEEE

Computer Society, 2005. Information Technology: Coding and Computing, International Conference. Apr. 4. 2005. Las Vegas, Nevada. – Pp. 586-591.

19. Messerges, T. Using Second-Order Power Analysis to Attack DPA Resistant Software. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-44499-8_19.pdf .
20. Quisquater, J.-J., Samyde, D. Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. Smart Cards Programming and Security (e-Smart 2001). Lectures Notes in Computer Science (LNCS). 2001. Vol. 2140. Springer. – Pp. 200—210.
21. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P. The EM Side Channel(s): Attacks and Assessment Methodologies. In Cryptographic Hardware and Embedded Systems // CHES 2002, LNCS 2523. Springer-Verlag. – Pp. 29–45.
22. Quisquater, J.-J., Samyde, D. Automatic Code Recognition for Smart Cards Using a Kohonen Neural Network. URL: https://www.usenix.org/legacy /event/cardis02/full papers/quisquater/quisquater.pdf.