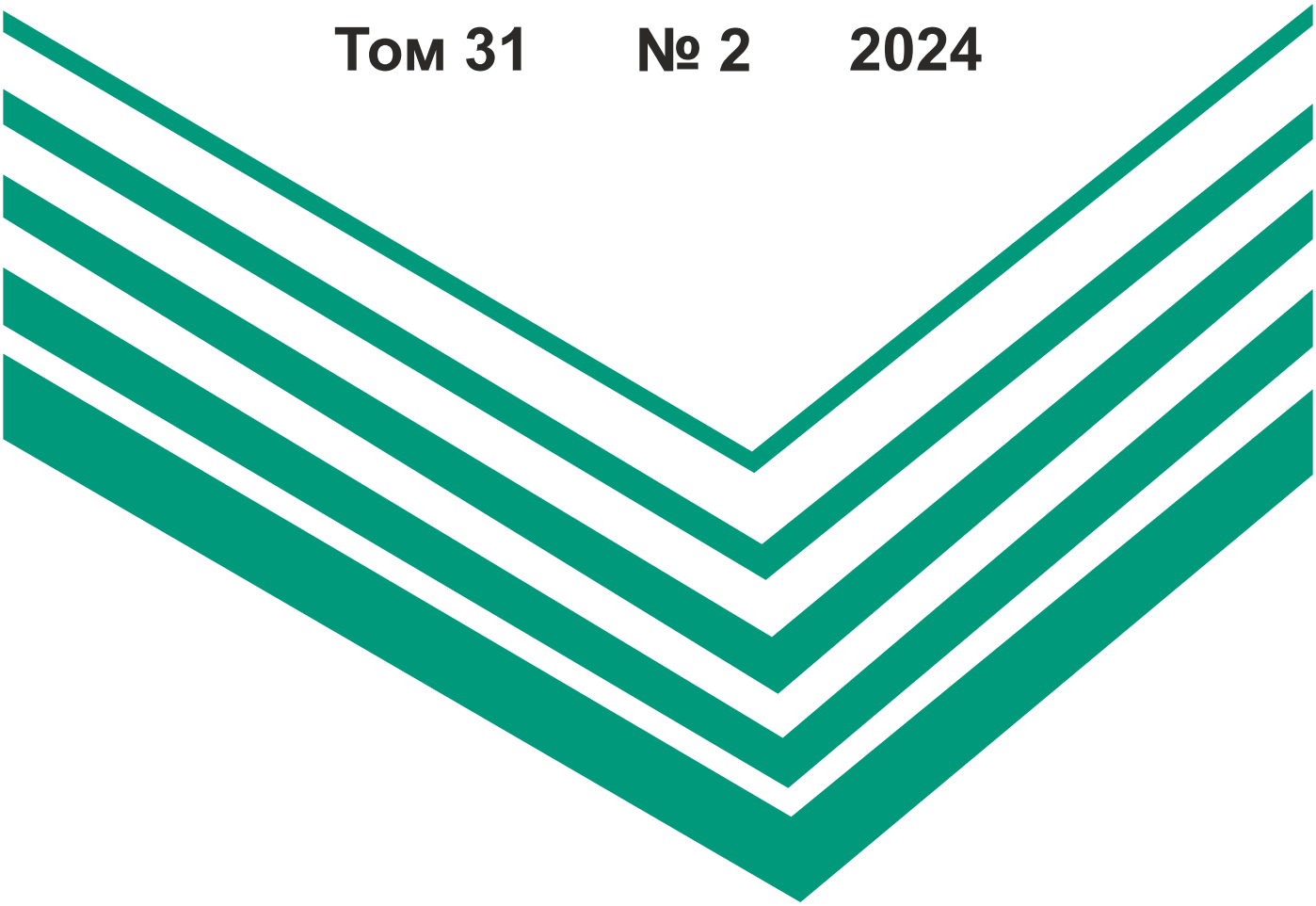
ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 31 № 2 2024



Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель–июнь 2024. Т. 31, № 2. С. 96–107

УДК 004.056.5 DOI: 10.33048/daio.2024.31.776

СПОСОБ ОПТИМАЛЬНОГО ИЗМЕРЕНИЯ ЗНАЧЕНИЙ НЕКОТОРЫХ ПАРАМЕТРОВ FAULT-АТАК НА КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Ю. А. Зуев [a], *П. Г. Ключарёв* [b]

Московский гос. технический университет им. Н. Э. Баумана,
ул. 2-я Бауманская, 5, 105005 Москва, Россия
E-mail: [a] 79851965730@yandex.ru, [b] pk.iu8@yandex.ru

Аннотация. Работа посвящена построению оптимального по времени способа измерения максимально допустимого (критического) значения напряжения питания (а также других параметров) устройства, на котором выполняется криптографический алгоритм. Знание этих величин необходимо для успешного проведения индуцирования ошибок в рамках проведения fault-атак. Способ построен на основе метода динамического программирования. Библиогр. 11.

Ключевые слова: fault-атака, динамическое программирование.

Введение

Один из важнейших классов атак по побочным каналам на практические реализации криптоалгоритмов — это так называемые fault-атаки или атаки по ошибкам вычислений [1–7]. Они основаны на индуцировании ошибок в работе аппаратных устройств, на которых выполняются криптографические алгоритмы. Эти ошибки приводят к искажениям информации, при анализе которых в ряде случаев можно восстановить секретный ключ. Индуцирование ошибок производится различными способами, среди которых можно назвать, в частности, воздействие магнитными и электромагнитными полями, высокой температурой, лазерным лучом и т. д. Пожалуй, наиболее распространённым является индуцирование ошибок с помощью изменения напряжения питания. Существенное повышение или понижение напряжения либо изменение напряжения по сложному закону часто способны индуцировать необходимые для проведения атаки ошибки. Во время практической реализации такой атаки необходимо знать максимальное напряжение, не приводящее к выходу устройства из строя. Назовём это напряжение критическим. Измерение критического напряжения может сводиться к постепенному увеличению

напряжения питания устройства с периодической проверкой его работоспособности. Не следует однако забывать, что при достижении критического напряжения устройство может выйти из строя далеко не мгновенно, поэтому процесс измерения критического напряжения может занять длительное время. Вместе с тем, если имеется несколько идентичных образцов устройства, то процесс измерения критического напряжения можно оптимизировать по времени.

В связи с изложенным рассмотрим следующую задачу. Пусть проводится измерение критического напряжения следующим образом. Рассматривается монотонно возрастающая конечная последовательность напряжений питания: $u_1, u_2, \ldots, u_n$. Если в процессе измерения мы готовы испортить только один образец устройства, то последовательно подавая на него напряжения $u_1, u_2, \ldots, u_i$ и зафиксировав выход устройства из строя при напряжении u_i, прекращаем испытания, установив тем самым, что критическое напряжение равно u_{i-1}.

При наличии одного образца — это единственный план проведения измерения критического напряжения. Его осуществление может потребовать n испытаний. Однако если имеется несколько идентичных опытных образцов, то максимальное число требуемых испытаний может быть уменьшено. Простейшим является случай, когда число опытных образцов потенциально не ограничено. При этом условии оптимальная стратегия состоит в выборе напряжения $u_{\lceil n/2 \rceil}$ с последующим переходом к бóльшим или меньшим напряжениям в зависимости от результата испытания и дальнейшими аналогичными дихотомиями. Такая стратегия включает $\lfloor \log_2 n \rfloor + 1$ испытаний, а для её осуществления потребуется $\lfloor \log_2 n \rfloor + 1$ опытных образцов.

Интерес представляет исследование промежуточных случаев, когда при ограниченном числе образцов k требуется найти $\min\max$(число испытаний), где $\min$ берётся по всем возможным стратегиям проведения испытаний, а $\max$ означает выбор для стратегии самого трудного для неё случая. Обозначим этот $\min\max$, зависящий от k и n, через $l_k(n)$. Наш предварительный анализ показывает, что $l_1(n) = n$ и $l_k(n) = \lfloor \log_2 n \rfloor + 1$, если $k \geqslant \lfloor \log_2 n \rfloor + 1$. Заметим также, что если каждое испытание занимает одну единицу времени, то $l_k(n)$ представляет собой полное время испытаний, и задача может быть сформулирована как минимизация времени испытаний.

С чисто математической точки зрения это задача оптимального определения монотонной функции, заданной на цепи высоты n (т. е. линейно упорядоченном множестве из n элементов) и принимающей два значения: 0 или 1. Своеобразие задачи заключается в том, что в процессе распознавания значение 1 (выход образца из строя) гарантированно не должно появиться более k раз.

В работе даётся эффективный алгоритм типа динамического программирования для получения оптимального плана испытаний для любых значений k и n. При $k = 2$ указана точная формула для $l_2(n)$, и найдена асимптотика для $l_k(n)$ при фиксированном k и $n \to \infty$. Практически все полученные результаты фактически основаны на том очевидном свойстве функции $l_k(n)$, что она является монотонно неубывающей функцией от n и монотонно невозрастающей функцией от k.

При построении оптимального плана будем опираться на принцип динамического программирования Ричарда Беллмана, согласно которому «оптимальное поведение обладает тем свойством, что, каковы бы ни были первоначальное состояние и решение в начальный момент, последующие решения должны составлять оптимальное поведение относительно состояния, получающегося в результате первого решения» [8]. Этот принцип широко применяется в различных областях [9–11]. Также будем использовать принцип балансировки трудоёмкости на двух ветвях испытания, возникающих при выходе и невыходе из строя образца, который можно описать следующим образом.

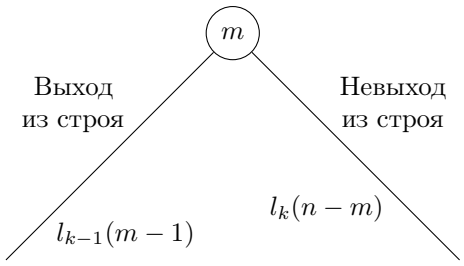


Рис. 1. Две ветви испытания

Как показано на рис. 1, если исследуется диапазон напряжений питания $u_1, u_2, \ldots, u_n$ и на испытываемый образец подаётся напряжение u_m, то в случае выхода образца из строя диапазон подлежащих дальнейшему исследованию напряжений становится равным $u_1, u_2, \ldots, u_{m-1}$, а число образцов уменьшается на единицу. Если же при подаче напряжения u_m образец не выходит из строя, то диапазон подлежащих дальнейшему исследованию напряжений становится равным $u_{m+1}, u_{m+2}, \ldots, u_n$, а число доступных для использования образцов остаётся неизменным. Тем самым в первом случае на выходе имеем $l_{k-1}(m-1)$, а во втором — $l_k(n-m)$.

При этом в оптимальном алгоритме шаг m в последовательности напряжений $u_1, u_2, \ldots, u_n$ должен быть выбран таким образом, чтобы минимизировать величину $\max\{l_{k-1}(m-1),\, l_k(n-m)\}$. Так как величина $l_j(i)$ при фиксированном j монотонно не убывает и с увеличением i на единицу может возрасти на единицу или остаться прежней, номер

напряжения m, при котором $l_{k-1}(m-1) = l_k(n-m)$, является оптимальным для выбора. В этом и состоит принцип балансировки трудоёмкости на двух ветвях испытания.

Здесь, однако, следует заметить, что точный баланс между ветвями не всегда может быть достигнут. Если для некоторого m имеет место $l_k(n-m) - l_{k-1}(m-1) = 1$ и при увеличении m на единицу $l_{k-1}(m-1)$ возрастает на единицу, а $l_k(n-m)$ на единицу убывает, то оказывается, что $l_k(n-m) - l_{k-1}(m-1) = -1$, и точного баланса добиться невозможно. В этом случае в оптимальном алгоритме может быть выбрано любое из двух значений: либо m, либо $m+1$.

1. Алгоритм построения оптимального плана

Для $l_k(n)$ имеем следующие очевидные граничные условия:

$$\begin{aligned} l_1(i) &= i, \quad i = 1, 2, \ldots, n; \\ l_i(1) &= 1, \quad i = 1, 2, \ldots, k. \end{aligned} \tag{1}$$

В основе алгоритма (см. алгоритм 1) лежит следующее рекуррентное соотношение:

$$l_k(n) = \min_{1 \leqslant m \leqslant \lceil n/2 \rceil} \max\{l_{k-1}(m-1),\, l_k(n-m)\} + 1, \tag{2}$$

где m — номер выбираемого при испытании напряжения u_m, $l_{k-1}(m-1)$ относится к ветви, связанной с выходом из строя образца, а $l_k(n-m)$ — с невыходом из строя. Диапазон проверяемых напряжений заканчивается на номере $\lceil n/2 \rceil$ ввиду того, что функция $l_k(n)$ при фиксированном k не убывает по n, а при фиксированном n не возрастает по k. Здесь и работает принцип балансировки между двумя ветвями.

Алгоритм 1. Построение оптимального плана

```
1: function OptimalPlan(n, k)
2:     for i = 1 to n do
3:         l_1(i) = i
4:     for i = 1 to k do
5:         l_i(1) = 1
6:     for i = 2 to k do
7:         for j = 2 to n do
8:             l_i(j) = min_{1 ⩽ m ⩽ ⌈j/2⌉} max{l_{i-1}(m-1), l_i(j-m)} + 1
```

С помощью равенства (2) и граничных условий (1) построчно заполняем $(k \times n)$-таблицу, последовательно вычисляя $l_i(j)$ для $i = 2, 3, \ldots, k$, $j = 2, 3, \ldots, n$. В каждую клетку (i, j) таблицы наряду со значением $l_i(j)$

заносится номер m напряжения питания u_m, которое следует использовать. Тем самым задаётся оптимальный план проведения исследования. Для любого числа используемых образцов $1 \leqslant i \leqslant k$ и длины $1 \leqslant j \leqslant n$ диапазона напряжений, которые могут возникнуть в ходе измерения, определено напряжение u_m, которое следует использовать, переходя затем к бóльшим или меньшим напряжениям в зависимости от результата испытания. Трудоёмкость алгоритма равна $O(kn^2)$ операций, так как заполнение каждой клетки таблицы требует $O(n)$ сравнений.

2. Определение $l_2(n)$

Примечательно, что в случае двух образцов оказывается возможным задать оптимальный план простой формулой, не прибегая к использованию приведённого выше алгоритма. Основная идея получения такой формулы также опирается на сбалансированность в оптимальном плане числа испытаний на двух ветвях алгоритма, получаемых при выходе и невыходе из строя опытного образца (рис. 2).

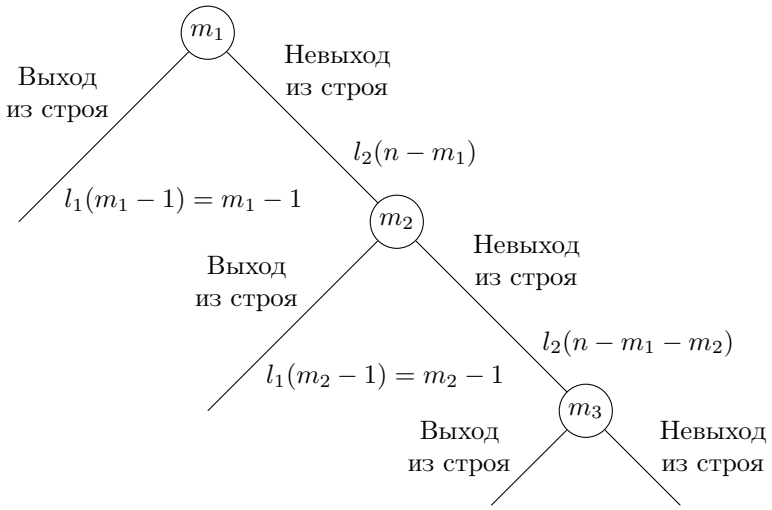


Рис. 2. Сбалансированность числа испытаний на ветвях алгоритма в случае двух образцов

Если для первого испытания выбрано напряжение с номером m_1, то при выходе образца из строя исследование будет продолжено со вторым образцом на напряжениях с номерами от 1 до m_1-1, которое может потребовать проведения $l_1(m_1-1)=m_1-1$ испытаний, а полное число испытаний окажется равным m_1. Если же образец не выйдет из строя, то исследование продолжится с двумя образцами на $n-m_1$ напряжениях

в диапазоне от u_{m_1+1} до u_n. При этом если для второго эксперимента выбирается напряжение с номером m_2 из нового диапазона, то в случае разрушения образца исследование будет проводиться со вторым образцом на напряжениях с номерами от 1 до $m_2 - 1$, которое может потребовать проведения $l_1(m_2 - 1) = m_2 - 1$ испытаний. Согласно принципу сбалансированности имеем $l_1(m_1 - 1) + 1 = l_1(m_2 - 1) + 2$, откуда $m_2 = m_1 - 1$.

Аналогично получаем, что $m_3 = m_2 - 1$, $m_4 = m_3 - 1$ и т. д., т. е. на каждом последующем испытании шаг уменьшается на единицу. Тем самым последовательность шагов по номерам напряжений питания выглядит следующим образом: m_1, $m_1 - 1$, $m_1 - 2$, ..., 1. Если очередной образец не выйдет из строя, то мы дойдём до нуля, и диапазон всех возможных напряжений будет исчерпан. Это позволяет записать для m_1 уравнение

$$\sum_{i=1}^{m_1} i = n. \tag{3}$$

Решением уравнения (3) является $m_1 = \sqrt{2n + 1/4} - 1/2$. Это число целое, если и только если число n треугольное, т. е. $n = \sum\limits_{i=1}^{k} i = k(k+1)/2$, так что $\sqrt{2n + 1/4} - 1/2 = k$. В этом случае при всех дальнейших ветвлениях число остающихся для исследования напряжений остаётся треугольным, и при каждом испытании при наличии двух образцов сохраняется точный баланс между двумя ветвями алгоритма. Если $n = k(k+1)/2+1$, то уже на первом шаге алгоритма точного баланса между ветвями достигнуть не удаётся, и трудоёмкость одной из ветвей вырастет на единицу, поэтому $l_2(k(k+1)/2 + 1) = k + 1$.

В общем случае при $k(k+1)/2 < n < (k+1)(k+2)$ из монотонности функции $l_2(n)$ следует, что равенство $l_2(n) = k + 1 = \lceil \sqrt{2n + 1/4} - 1/2 \rceil$ сохраняется, поэтому число испытаний равно $l_2(n) = \lceil \sqrt{2n + 1/4} - 1/2 \rceil$. Такой же номер напряжения следует выбирать при первом испытании, действуя аналогично при последующих испытаниях в случае невыхода образца из строя. Таким образом, доказано

Утверждение 1. *В случае двух образцов и n напряжений в последовательности оптимальное число испытаний равно $\lceil \sqrt{2n + 1/4} - 1/2 \rceil$, и такой же шаг нужно делать по диапазону номеров исследуемых напряжений при каждом испытании с двумя образцами, когда текущий диапазон исследуемых напряжений питания состоит из n элементов.*

3. Нахождение асимптотики $l_k(n)$ при $n \to \infty$

Точные формулы для $l_k(n)$, по-видимому, были бы слишком сложными. Однако, качественное представление о зависимости числа испытаний

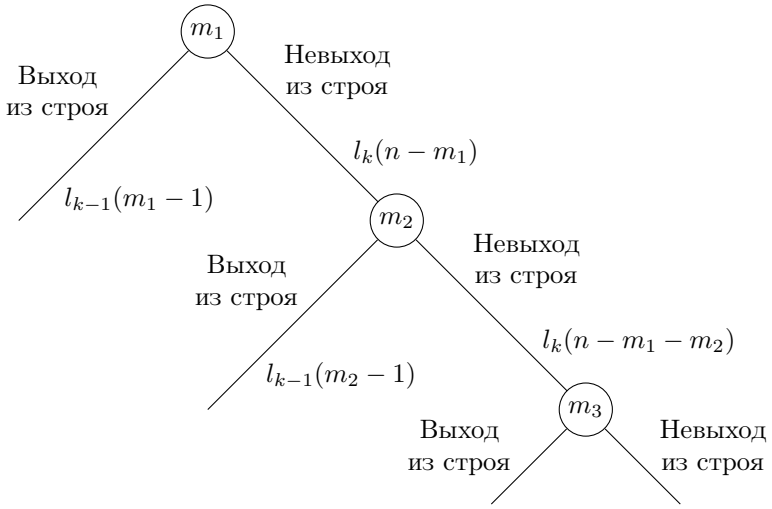


Рис. 3. Сбалансированность числа испытаний
на ветвях алгоритма в общем случае

от числа имеющихся образцов можно получить, ограничившись асимптотическими оценками. Докажем, что число необходимых испытаний $l_k(n)$ при фиксированном числе k опытных образцов и числе возможных различных напряжений питания $n \to \infty$ асимптотически равно

$$l_k(n) \sim \sqrt[k]{k!n}, \quad n \to \infty. \tag{4}$$

Доказательство проведём индукцией по числу k опытных образцов. При $k = 1, 2$ утверждение, очевидно, справедливо. Пусть оно справедливо для k опытных образцов, т. е. имеет место (4). Докажем его справедливость для $k+1$ опытных образцов, т. е. покажем, что

$$l_{k+1}(n) \sim \sqrt[k+1]{(k+1)!n}, \quad n \to \infty.$$

Как и прежде, будем опираться на равенство числа испытаний в случаях выхода из строя и невыхода из строя образца (рис. 3).

Рассмотрим два возможных пути по дереву испытаний на рис. 3. В первом случае на первом же шаге при подаче напряжения u_{m_1} образец выходит из строя. Во втором случае образец выдерживает напряжение u_{m_1} и выходит из строя на втором шаге при подаче напряжения $u_{m_1+m_2}$. Тогда, как следует из принципа сбалансированности, при оптимальном выборе m_1 и m_2 должно выполняться равенство

$$l_k(m_1-1) + 1 = l_k(m_2-1) + 2,$$

т. е.

$$l_k(m_1-1) - l_k(m_2-1) = 1.$$

Аналогичное соотношение справедливо и для всех последующих выборов напряжения

$$l_k(m_i - 1) - l_k(m_{i+1} - 1) = 1.$$

(В асимптотическом анализе возможными нарушениями баланса пренебрегаем.)

Последним является $l_{k+1}(n)$-е испытание, в котором $m_{l_{k+1}(n)} = 1$, следовательно, $l(m_{l_{k+1}(n)} - 1) = 0$. Отсюда получаем

$$\begin{gathered} l_k(m_{l_{k+1}(n)} - 1) = 0; \\ l_k(m_{l_{k+1}(n)-1} - 1) = 1; \\ l_k(m_{l_{k+1}(n)-2} - 1) = 2; \\ \cdots\cdots\cdots\cdots \\ l_k(m_1 - 1) = l_{k+1}(n) - 1. \end{gathered} \tag{5}$$

Согласно (4) имеем $l_k(m_i - 1) \sim \sqrt[k]{k!(m_i - 1)}$, значит,

$$m_i \sim m_i - 1 \sim \frac{l_k^k(m_i - 1)}{k!}, \quad m_i \to \infty. \tag{6}$$

Далее имеем очевидное соотношение

$$\sum_{i=1}^{l_{k+1}(n)} m_i = n. \tag{7}$$

Из (5)–(7) выводим

$$\begin{aligned} n = \sum_{i=1}^{l_{k+1}(n)} m_i \sim \sum_{i=1}^{l_{k+1}(n)} \frac{l_k^k(m_i - 1)}{k!} \sim \frac{1}{k!} \sum_{i=1}^{l_{k+1}(n)-1} i^k \\ \sim \frac{1}{k!} \int_0^{l_{k+1}(n)} x^k dx = \frac{l_{k+1}^{k+1}(n)}{(k+1)!}, \quad n \to \infty. \end{aligned} \tag{8}$$

Из (8) получаем требуемое асимптотическое соотношение

$$l_{k+1}(n) \sim \sqrt[k+1]{(k+1)!n}, \quad n \to \infty.$$

Утверждение 2. *При фиксированном числе k изначально имеющихся образцов и числе различных напряжений питания $n \to \infty$ оптимальное число испытаний асимптотически равно $\sqrt[k]{k!n}$, и асимптотически такой же шаг нужно делать по диапазону исследуемых напряжений, содержащему n элементов.*

Заключение

В работе представлен эффективный алгоритм типа динамического программирования для составления оптимального плана испытаний при определении критического напряжения питания, необходимого в процессе планирования fault-атак. В случае двух имеющихся образцов получены точные формулы для проведения оптимального по времени измерения, делающие в этом случае ненужным использование алгоритма. В общем случае полученные асимптотические формулы дают качественное представления о том, как увеличение числа образцов уменьшает число необходимых испытаний. В основе всех полученных результатов лежит последовательно используемый принцип балансировки.

Полученные результаты могут применяться также в задачах поиска максимально допустимых значений других величин, использующихся в задачах индуцирования ошибок для проведения fault-атак, например, температуры, напряжённости электромагнитного поля и др. Кроме того, они могут оказаться востребованными и в иных, отличных от криптоанализа, сферах, когда требуется найти силу разрушающего воздействия на изделие, для которого имеются несколько образцов.

Финансирование работы

Исследование выполнено в рамках стратегического проекта DeepAnalytics программы «Приоритет 2030». Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Baksi A., Bhasin S., Breier J., Jap D., Saha D.** A survey on fault attacks on symmetric key cryptosystems // ACM Comput. Surveys. 2022. V. 55, No. 4. Paper ID 86. 34 p.
2. **Breier J., Jap D.** A survey of the state-of-the-art fault attacks // Proc. 14th Int. Symp. Integrated Circuits (Singapore, Dec. 10–12, 2014). Piscataway: IEEE, 2014. P. 152–155.
3. **Giraud C., Thiebeauld H.** A survey on fault attacks // Smart card research and advanced applications VI. IFIP 18th World Computer Congress. TC8/WG8.8 & TC11/WG11.2 6th Int. Conf. (Toulouse, France, Aug. 22–27, 2004) New York: Kluwer Acad. Publ., 2004. P. 159–176.
4. **Kim C. H., Quisquater J.-J.** Faults, injection methods, and fault attacks // IEEE Des. Test Comput. 2007. V. 24, No. 6. P. 544–545.
5. **Gangolli A., Mahmoud Q. H., Azim A.** A systematic review of fault injection attacks on IoT systems // Electronics. 2022. V. 11, No. 13. Paper ID 2023. 24 p.

6. **Piscitelli R., Bhasin S., Regazzoni F.** Fault attacks, injection techniques and tools for simulation // Hardware security and trust. Design and deployment of integrated circuits in a threatened environment. Cham: Springer, 2017. P. 27–47.
7. **Shepherd C., Markantonakis K., van Heijningen N., Aboulkassimi D., Gaine C., Heckmann T., Naccache D.** Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis // Comput. Secur. 2021. V. 111. Paper ID 102471. 31 p.
8. **Беллман Р.** Динамическое программирование. М.: Изд-во иностр. лит-ры, 1960. 400 с.
9. **Dreyfus S.** The art and theory of dynamic programming. New York: Acad. Press, 1977. 284 p. (Math. Sci. Eng.; V. 130).
10. **Lew A., Mauch H.** Dynamic programming: A computational tool. Heidelberg: Springer, 2010. 379 p.
11. **Cormen T. H., Leiserson C. E., Rivest R. L., Stein C.** Introduction to algorithms. Cambridge, MA: MIT Press, 2022. 1312 p.

Зуев Юрий Анатольевич
Ключарёв Пётр Георгиевич

Статья поступила
4 июня 2023 г.
После доработки —
9 октября 2023 г.
Принята к публикации
22 декабря 2023 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
April–June 2024. Vol. 31, No. 2. P. 96–107

UDC 004.056.5 DOI: 10.33048/daio.2024.31.776

A METHOD FOR OPTIMAL VALUE MEASUREMENT OF SOME PARAMETERS OF FAULT ATTACKS ON CRYPTOGRAPHIC ALGORITHMS

Yu. A. Zuev[a] and *P. G. Klyucharev*[b]

Bauman Moscow State Technical University,
5 Vtoraya Baumanskaya Street, 105005 Moscow, Russia
E-mail: [a]79851965730@yandex.ru, [b]pk.iu8@yandex.ru

Abstract. This paper is devoted to the construction of a time-optimal method for measuring the maximum permissible (critical) value of the supply voltage (as well as other parameters) of the device on which the cryptographic algorithm is performed. Knowledge of these values is necessary for successful conduct of error injection, as part of a fault attack. The method is based on dynamic programming. Bibliogr. 11.

Keywords: fault-attack, dynamic programming.

References

1. **A. Baksi, S. Bhasin, J. Breier, D. Jap,** and **D. Saha,** A survey on fault attacks on symmetric key cryptosystems, *ACM Comput. Surveys* **55** (4), Paper ID 86 (2022).
2. **J. Breier** and **D. Jap,** A survey of the state-of-the-art fault attacks, in *Proc. 14th Int. Symp. Integrated Circuits, Singapore, Dec. 10–12, 2014* (IEEE, Piscataway, 2014), pp. 152–155.
3. **C. Giraud** and **H. Thiebeauld,** A survey on fault attacks, in *Smart Card Research and Advanced Applications VI* (IFIP 18th World Computer Congress. TC8/WG8.8 & TC11/WG11.2 6th Int. Conf., Toulouse, France, Aug. 22–27, 2004) (Kluwer Acad. Publ., New York, 2004), pp. 159–176.
4. **C. H. Kim** and **J.-J. Quisquater,** Faults, injection methods, and fault attacks, *IEEE Des. Test Comput.* **24** (6), 544–545 (2007).
5. **A. Gangolli, Q. H. Mahmoud,** and **A. Azim,** A systematic review of fault injection attacks on IoT systems, *Electronics* **11** (13), Paper ID 2023 (2022).

English transl.: *Journal of Applied and Industrial Mathematics* **18** (2), 371–377 (2024), DOI: 10.1134/S1990478924020182.

6. **R. Piscitelli, S. Bhasin,** and **F. Regazzoni,** Fault attacks, injection techniques and tools for simulation, in *Hardware Security and Trust. Design and Deployment of Integrated Circuits in a Threatened Environment* (Springer, Cham, 2017), pp. 27–47.
7. **C. Shepherd, K. Markantonakis, N. van Heijningen, D. Aboulkassimi, C. Gaine, T. Heckmann,** and **D. Naccache,** Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis, *Comput. Secur.* **111**, Paper ID 102471 (2021).
8. **R. Bellman,** *Dynamic Programming* (Princeton Univ. Press, Princeton, NJ, 1957; Izd. Inostr. Lit., Moscow, 1960 [Russian]).
9. **S. Dreyfus,** *The Art and Theory of Dynamic Programming* (Acad. Press, New York, 1977) (Math. Sci. Eng., Vol. 130).
10. **A. Lew** and **H. Mauch,** *Dynamic Programming: A Computational Tool* (Springer, Heidelberg, 2010).
11. **T. H. Cormen, C. E. Leiserson, R. L. Rivest,** and **C. Stein,** *Introduction to Algorithms* (MIT Press, Cambridge, MA, 2022).

Yury A. Zuev
Petr G. Klyucharev

Received June 4, 2023
Revised October 9, 2023
Accepted December 22, 2023