МЕТОДЫ ЗАЩИТЫ ОТ АТАК ПО ПОБОЧНЫМ КАНАЛАМ АППАРАТНОЙ РЕАЛИЗАЦИИ СХЕМ ПОСТКВАНТОВОЙ ПОДПИСИ, ПОСТРОЕННЫХ НА ОСНОВЕ ПРОТОКОЛА ИДЕНТИФИКАЦИИ ШТЕРНА

Смирнов Д. К.[1], Чижов И. В.[2]

DOI: 10.21681/2311-3456-2025-3-21-28

Цель исследования: *разработка протокола идентификации Штерна, устойчивого к атакам по побочным каналам.*

Метод(ы) исследования: *изучение современных методов атак на криптографические схемы со схожими вычислительными элементами, способов защиты от этих атак, модификация схемы с целью защиты приватного ключа при краже токена.*

Результат(ы) исследования: *выделены уязвимые вычислительные элементы протокола – сложение векторов по модулю 2 и умножение матрицы на вектор – и проанализированы основные методы защиты этих элементов от утечек по побочным каналам, такие как маскирование, балансирование и перемешивание. Предложен способ матричного умножения, устойчивый к горизонтальной корреляционной атаке, применявшейся против криптосистемы Мак-Элиса. Установлены основные требования к реализации схемы на ПЛИС, предложена модификация схемы с маскированием ключа, не нарушающая стойкость оригинальной, позволяющая защитить секрет при краже токена и предотвращающая атаки имперсонализации благодаря маскированию. Способ генерации маски выбран таким образом, чтобы минимизировать место, занимаемое на ПЛИС, а именно хэширование парольной фразы функцией «Стрибог-К» со счётчиком. Показано, что стойкость модифицированного протокола идентификации Штерна совпадает со стойкостью оригинального протокола в модели без утечек по побочным каналам и превосходит в модели с ними.*

Научная новизна: *результаты работы позволяют реализовать постквантовый алгоритм подписи «Шиповник», разрабатываемый рабочей группой ТК26 и проходящий стандартизацию в настоящее время.*

Ключевые слова: *синдромное декодирование, схема подписи «Шиповник», корреляционная атака, атака по электромагнитному излучению, атака по энергопотреблению, атака с внесением ошибок.*

Введение

В ответ на возрастающую угрозу построения квантового компьютера множество исследователей посвящают себя изучению и развитию постквантовой криптографии. В частности, силами рабочей группы ТК26 разрабатывается постквантовый алгоритм подписи «Шиповник», основанный на протоколе идентификации Штерна.

Известно, что идеальная математическая абстракция существует лишь в теоретическом мире. При реализации криптографических алгоритмов легко допустить ошибку, способную уничтожить всю теоретическую стойкость. Классические ЭВМ работают благодаря электричеству, которое, проходя по проводнику, способно менять окружающее электромагнитное поле. Изменение данных на регистрах устройства требует более высокого энергопотребления. Всё это может нести информацию о секретных данных, нарушая секретность по Шеннону. Именно этим и пользуются злоумышленники, проводя атаки по побочным каналам.

Эти атаки можно провести без использования квантового компьютера на классическом вычислителе. Поэтому данная работа ставит конечной целью разработку протокола идентификации Штерна как основной части алгоритма подписи «Шиповник» на ПЛИС таким образом, чтобы она была устойчивой к атакам по побочным каналам.

Вопрос реализации протокола Штерна, устойчивой к атакам по побочным каналам, уже изучался в работе [22]. Однако подход, предложенный в ней, требует дважды вычислять матричное умножение, причём алгоритм этого умножения подвержен утечкам, генерировать маску для каждого раунда протокола и предполагает хранение приватного ключа на устройстве без маски. В этой статье предлагается устойчивый к данному типу атак вариант матричного умножения, который требуется вычислить только один раз, а модифицированная версия протокола позволяет хранить и проводить вычисления над приватным ключом в маскированном виде.

1 Смирнов Дмитрий Константинович, магистр, МГУ имени М. В. Ломоносова, АО «ИнфоТеКС», г. Москва, Россия. E-mail: s02190708@stud.cs.msu.ru

2 Чижов Иван Владимирович, кандидат физико-математических наук, доцент, МГУ имени М. В. Ломоносова, Федеральный исследовательский центр «Информатика и управление» РАН, АО «НПК «Криптонит», г. Москва, Россия. E-mail: ichizhov@cs.msu.ru

Описание протокола идентификации Штерна

Протокол идентификации Штерна – интерактивный протокол с нулевым разглашением, предложенный Ж. Штерном в 1993 году [1]. Его стойкость основана на сложности задачи синдромного декодирования. Пусть выбрана некоторая хэш-функция $h(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^l$. Выбран также код, исправляющий ошибки, длины n, размерности k, с кодовым расстоянием ω. Матрица $H \in \{0,1\}^{(n-k)\times n}$ – его проверочная матрица, $s = \{0,1\}^n$ – приватный ключ подписывающего абонента P, $y = Hs^T$ – его публичный ключ. Слово $A\|B$ – конкатенация слов A и B. Абонент P (Prover) выбирает случайное n-битное слово u и случайную перестановку σ на множестве целых чисел $\{1..n\}$, вычисляет:

$$c_0 = h(\sigma\|Hu^T)$$
$$c_1 = h(\sigma(u))$$
$$c_2 = h(\sigma(u \oplus s))$$

и отправляет c_0, c_1, c_2 проверяющему абоненту V (Verifier).

Абонент V выбирает случайное число $b \in \{0,1,2\}$ и посылает абоненту P. На основании b абонент P раскрывает некоторую пару значений абоненту V:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus s$;
если $b = 2$, то $r_0 = \sigma(u)$, $r_1 = \sigma(s)$.

Последним шагом V проверяет равенства:

если $b = 0$, то $c_0 = h(r_0\|Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если b = 1, то $c_0 = h(\sigma\|Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$;
если b = 2, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Если они оказываются верными, абонент P считается идентифицированным.

Противник без знания секретного ключа может успешно пройти проверку с вероятностью 2/3, поэтому необходимо повторять протокол k раз. Это влечёт за собой нагрузку на сеть из-за большого количества пересылок между абонентами. Решением этой проблемы может быть применение преобразования Фиата-Шамира [2, 3].

Модели утечек

Как правило, рассматриваются 2 модели утечек:

1) Модель расстояния Хэмминга. Она основана на предположении, что потребляемая мощность зависит от расстояния Хэмминга $\rho_H(x_{old}, x_{new})$ между старым x_{old} и новым x_{new} значением на шине.
2) Модель веса Хэмминга. Является частным случаем предыдущей модели с допущением, что старое значение было нулевым:

$$\rho(0, x_{new}) = wt(0 \oplus x_{new}) = wt(x_{new}), \quad (1)$$

где $wt(\cdot)$ – вес Хэмминга.

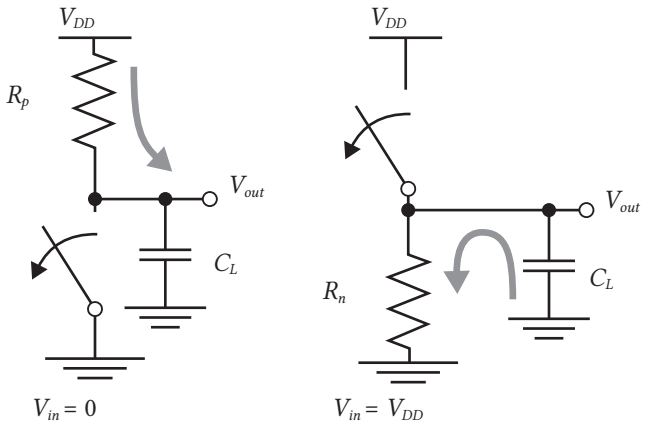

Рис. 1. КМОП-инвертор [5]

Атаки по энергопотреблению

Большинство ПЛИС используют память, реализуемую на КМОП (см. рис. 1). Особенность такой памяти заключается в том, что на статичное хранение информации энергии требуется значительно меньше, чем на её изменение. Это объясняется тем, что когда состояние схемы не меняется, между источником питания и землёй закрыт хотя бы один транзистор. Таким образом, КМОП вентиль имеет мощность рассеивания порядка 0,01 мВ в статичном состоянии, 1 мВ и 5 мВ при изменении состояния на частотах 1 МГц и 10 МГц соответственно [4].

Именно эта особенность и даёт возможность отследить изменения данных на шине. За один такт перехода из разряженного в заряженное состояние и обратно «идеальной» КМОП схемой потребляется энергия:

$$E_s = C_L V_{DD}^2, \quad (2)$$

где C_L – ёмкость нагрузки транзистора, V_{DD} – напряжение источника питания. На практике энергия зарядки и разрядки может различаться, так как эти процессы происходят в разных элементах схемы – n-МОП и p-МОП транзисторах. Они могут обладать разными ёмкостями и сопротивлением [5].

Рассмотрим метод корреляционной атаки, использующей замеры энергопотребления, описанный в [6]. В качестве функции шифрования используют сложение по модулю 2. Атакующий строит предположение о наборе вероятных значений секрета на некотором этапе криптографического алгоритма. Выбрав за модель утечек модель расстояния Хэмминга, вычисляет

$$H_{i,R} = wt(M_i \oplus R), \quad (3)$$

где R – неизвестное предыдущее состояние регистра, а M_i – некоторые известные данные. Далее вычисляет коэффициенты корреляции между набором измерений W_i и набором предположений $H_{i,R}$:

$$\rho_{WH}(R) = \frac{N\sum W_i H_{i,R} - \sum W_i \sum H_{i,R}}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\,\sqrt{N\sum H_{i,R}^2 - (\sum H_{i,R})^2}}, \quad (4)$$

где N – размер каждого из наборов, а суммирование проводится от 1 до N. Перебирая R и вычисляя значение $\rho_{WH}(R)$ для каждого из них, атакующий находит такое R, которое даёт максимальный коэффициент корреляции.

Как утверждает П. Кохер и др. в [7], для защиты от анализа энергопотребления стоит реализовывать алгоритм таким образом, чтобы в программе не было ветвлений, балансировать вес Хэмминга переменных значений (на регистрах или шине) и физически экранировать устройство. Хотя все эти меры и не смогут полностью исключить возможность успешной атаки.

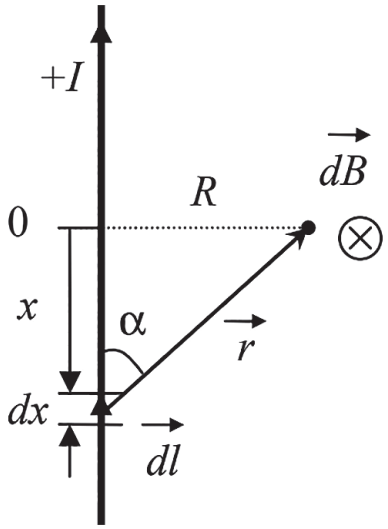

Рис. 2. Иллюстрация закона Био-Савара-Лапласа

Атаки по электромагнитному излучению

Хорошо известен закон Био-Савара-Лапласа (см. рис. 2), определяющий вектор индукции магнитного поля, порождаемого постоянным электрическим током:

$$d\vec{B} = \frac{\mu_0}{4\pi}\frac{I[d\vec{l} \times \vec{r}]}{r^3}, \quad (5)$$

где μ_0 – магнитная постоянная, I – ток в проводнике, $d\vec{l}$ – элемент проводника, $\vec{r}$ – радиус-вектор от элемента проводника до точки, в которой измеряется индукция магнитного поля. Направление $d\vec{B}$ перпендикулярно плоскости, в которой лежат $d\vec{l}$ и $\vec{r}$, и определяется правилом правого винта.

При зарядке и разрядке КМОП инвертора происходит движение электронов. Причём, в первом случае оно имеет одно направление, а в другом – противоположное (см. рис. 1). Тот факт, что направление вектора магнитной индукции будет зависеть от направления тока, даёт возможность определить характер изменения состояния схемы: с 0 на 1 или с 1 на 0.

Э. Питерс и др. исследовали возможность такой атаки [8]. Хотя такой способ позволяет не подключаться к сети напрямую, он более сложный в исполнении. Авторы использовали маленькую пружинку, которую нужно было разместить точно над шиной. Для этого может потребоваться микроскопическое исследование схемы ПЛИС.

Атаки с внесением ошибок

Эти атаки изучались во множестве работ [9–12]. Самые простые варианты атак заключаются в изменении напряжения питания, добиваясь сбоев в синхронизирующем сигнале CLK, более сложные требуют использования лазера, успешность которых опирается на эффект ионизации элементов КМОП. С этой проблемой сталкиваются, например, спутники, попадающие под ионизирующее излучение Солнца. По этой причине в спутниках используются коды Рида-Соломона [13].

Контролируемое внесение лазером ошибок в криптографические алгоритмы позволяют использовать дифференциальный анализ [14].

Корреляционная атака на криптосистему Мак-Элиса

В 2023 году была опубликована атака на криптосистему Мак-Элиса, использующая данные энергопотребления во время вычисления синдрома секретного вектора ошибки $H_{pub}e = s$ [15]. Выше была описана общая схема атаки, которой придерживались и авторы указанной статьи. Они искали корреляцию измерений со столбцами матрицы H_{pub}: если в e на позиции i стоит единица, на результирующую сумму повлияет i-тый столбец H_{pub}, а значит изменится и состояние регистра с промежуточным результатом. После сортировки массива коэффициентов корреляции по убыванию отбираются первые t элементов, соответствующих некоторым наиболее вероятным столбцам. Поскольку при реальном проведении атаки во время замеров неизбежно будут шумы, может произойти ошибка, и на самом деле вместо единицы на какой-то позиции будет стоять 0. А из условия $wt(e) = t$ следует, что «пропавшая» единица должна соответствовать элементу из оставшихся $n - t$.

В связи с этим авторы использовали подход, являющийся развитием предложенного Ю. Пранджем [16], который позволяет смягчить требование к столбцам матрицы H_{pub}: t столбцов, соответствующих единицам в e, не обязаны быть первыми t столбцами, а могут находиться среди первых $n - k$ столбцов.

Балансирование

Согласно работе [7], балансирование веса Хэмминга на регистрах может быть эффективным способом защиты. Однако в статье [17] приводится аргумент против такого метода: вычисление балансирующего значения будет немного сдвинуто по времени, и злоумышленник сможет манипулировать внешними условиями (такими, как напряжение питания), чтобы увеличить этот отрезок времени.

Перемешивание

Другим популярным способом защиты является перемешивание независящих друг от друга операций, например, чтение S-box'ов DES в случайном порядке. То есть, если один из них будет прочитан первым с вероятностью 1/8, то усреднив 64 запуска атаки можно получить исходный сигнал и обойти защиту [17].

Маскирование

Суть этого метода заключается в том, что на регистрах хранят данные не в открытом виде, а в преобразованном:

$$x = x_1 \circ x_2 \circ \ldots \circ x_d, \quad (6)$$

где x – преобразованный секрет, $\circ$ – некоторая групповая операция, а набор x_i называется набором долей. Как правило, в качестве групповой операции подразумевается сложение по модулю 2, за x_1 берут секрет, а за остальные доли – маски. При анализе атак по побочным каналам на криптосистему NTRU, другого кандидата на постквантовый криптографический стандарт, маскирование секретного ключа оказалось наиболее эффективным способом защиты среди различных перемешиваний и маскирования шифртекста [18]. Более того, стойкость этого метода можно доказать [19].

Теневой регистр

Автор во время исследования существующего опыта обнаружил лишь попытки маскировать регистр, на котором содержится секретный вектор e, во время вычисления $H_{pub}e = s$, но не нашёл предложений складывать не только столбцы, соответствующие единицам, но и нулям: тогда атаки по энергопотреблению с корреляционным анализом, например, из [15], окажутся неэффективными. Рассмотрим кратко идею.

Будем читать секретный вектор e по битам. Если очередной бит e_i равен нулю, то i-тая строка H_{pub} складывается с регистром reg_0, иначе – с reg_1. Оба регистра инициализированы нулём. В итоге мы используем все строки матрицы независимо от секретного вектора. В качестве результата такого умножения вектора на матрицу выдаём reg_1.

Замеры энергопотребления не будут зависеть от секрета. Но если у злоумышленника удастся разместить пробирующую пружинку, как это сделали в [8], точно над регистром reg_1, то он заметит области, в которых электромагнитное поле почти не изменяется, – это будут строки, соответствующие нулям. Поэтому, хотя это и довольно сильное предположение, одного метода защиты недостаточно.

Маскирование ключа

Секретный ключ будет храниться в маскированном виде и все вычисления над ним будут проводиться с той же маской. Маска вырабатывается из пароля, который известен пользователю. Для этого можно воспользоваться хэш-функцией «Стрибог-K». Уже доказано, что «Стрибог» неразличим от случайного оракула в модели идеального блочного шифра, то есть, является псевдослучайной функцией [20]. А из псевдослучайной функции можно построить псевдослучайный генератор [21].

Что может позволить такая конструкция? Дело в том, что большинство рассмотренных атак требуют физического доступа к устройству. Предполагая, что противник обладает возможностями по внесению ошибок, замерам напряжения или электромагнитного излучения, или, даже в более сильных предположениях, прочитать хранящиеся значения в памяти ПЛИС, секретный ключ может быть раскрыт противником. Более того, существует угроза подписи им сообщений даже при неизвестном ключе, для чего ему не требуется проведения никаких атак. Однако если ключ дополнительно будет маскирован с помощью пароля, это сильно затруднит реализацию угроз.

Сейчас нам требуется изменить вычислительный алгоритм таким образом, чтобы алгоритм самого протокола не изменился, но стал учитывать вышеописанные рассуждения. Пусть мы получаем пароль $Pass \in \{0,1\}^t$, $t < 512$ и генерируем из него маску $M = F(Pass) \in \{0,1\}^n$. Абонент P обладает маскированным ключом $s' = s \oplus M$. Теперь ему требуется вычислить

$$u' = u \oplus M;$$
$$c_0 = h(\sigma \| Hu'^T),$$
$$c_1 = h(\sigma(u')),$$
$$c_2 = h(\sigma(u \oplus s')) = h(\sigma(u' \oplus s)).$$

На основании выбора абонента V вернуть:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u'$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus s' = u' \oplus s$;
если $b = 2$, то $r_0 = \sigma(u')$, $r_1 = \sigma(s') \oplus \sigma(M) = \sigma(s)$.

Для получения открытого ключа вычисляется $y = Hs'^T \oplus HM^T = Hs^T$. Теперь можно заметить, что над секретным ключом не проводятся вычисления без маски.

Генерация маски

Ключ, по имеющимся на данный момент оценкам [3], имеет длину 2896 бит, что превышает длину хэш-функции «Стрибог-512» более, чем в 5 раз. Поэтому вычисления одного хэша будет недостаточно. Если каждый последующий блок будет зависеть лишь от предыдущего, злоумышленник сможет воспользоваться особенностью ключа, а именно его малым весом. Если предположить, что в первом 512-битном блоке не содержится ни одной единицы, то первые 512 бит s' представляют собой сам хэш. Если противник сможет извлечь весь вектор s', то ему будет

достаточно продолжить хэширование со второго блока, используя первый, и тогда он сможет восстановить секретный ключ. Поэтому каждый блок должен зависеть от пароля и не быть одинаковым. Например, можно использовать «Стрибог-K» с сообщением-счётчиком, равным номеру блока.

В части «Матричное умножение» была освещена атака с восстановлением ключа. Однако она требует физического доступа к устройству и вычислений с известным ключом (который в данном случае является паролем $Pass$). Но при известном пароле злоумышленнику не нужна эта атака, поскольку он сможет самостоятельно сгенерировать маску M.

Стратегии противника

Рассмотрим возможные стратегии злоумышленника для обмана абонента V.

Стратегия 0: нечестный доказывающий предполагает, что $b \neq 0$. Он выбирает $t = \{0,1\}n$, $wt(t) = \omega$.

$$c_0 = h(\sigma \| H(u \oplus t)^T \oplus y);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus t$;
если $b = 2$, то $r_0 = \sigma(u)$, $r_1 = \sigma(t)$.

Если предположение верно, проверяющий будет обманут:

если $b = 1$, то $c_0 = h(\sigma \| Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$;
если $b = 2$, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Стратегия 1: нечестный доказывающий предполагает, что $b \neq 1$. Он выбирает $t = \{0,1\}^n$, $wt(t) = \omega$.

$$c_0 = h(\sigma \| Hu^T);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если b = 2, то $r_0 = \sigma(u)$, $r_1 = \sigma(t)$.

Если предположение верно, проверяющий будет обманут:

если $b = 0$, то $c_0 = h(\sigma \| Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если $b = 2$, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Стратегия 2: нечестный доказывающий предполагает, что $b \neq 2$. Он выбирает $t = \{0,1\}^n$: $Ht^T = y$. Заметим, что в этом случае противник надеется, что проверки на вес не будет, поэтому достаточно найти любое подходящее решение, что можно сделать, например, методом Гаусса.

$$c_0 = h(\sigma \| Hr^T);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus t$.

Если предположение верно, проверяющий будет обманут:

если $b = 0$, то $c_0 = h(\sigma \| Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если $b = 1$, то $c_0 = h(\sigma \| Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$.

Стойкость модифицированной схемы

Будем называть $SC_1{:}T_1 \longrightarrow s$ и $SC_2{:}(T_1,T_2) \longrightarrow (s',M)$ такие машины Тьюринга, которые получают на вход наборы различных измерений напряжения и электромагнитного излучения, полученных в ходе работы устройства честного доказывающего абонента P, и возвращающие предполагаемый приватный ключ и маску. T_1 содержит информацию о приватном ключе, T_2 – о маске.

Первая машина соответствует оригинальному алгоритму Штерна, вторая – модифицированному. Пусть T_{SC_1}, T_{SC_2} – их время работы в тактах. Так как второй машине требуется вычислить помимо ключа ещё и маску, не умаляя общности, можно считать, что SC_1 содержится в SC_2 и

$$T_{SC_1} < T_{SC_2}. \quad (7)$$

Назовём $A = (A_1,A_2)$ машину Тьюринга, успешно обманывающую честного проверяющего абонента V в оригинальной схеме идентификации Штерна за T_A тактов. Машина состоит из двух частей, каждая из которых соо тветствует одному из шагов схемы.

$A(u,\sigma,y,b,\hat{b},s)$:
$(c_0,c_1,c_2,r_0',r_1',r_0'',r_1'') \longleftarrow A_1\,(u,\sigma,y,\hat{b},s)$,
$(r_0,r_1) \longleftarrow A_2\,(b,\hat{b},r_0',r_1',r_0'',r_1'')$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

Здесь и далее используются величины: $\hat{b}$ – выбор стратегии противника; r_0', r_1', r_0'', r_1'' – наборы ответов противника, соответствующие выбранной им стратегии.

Назовём $B = (B_1,B_2)$ машину Тьюринга, успешно обманывающую честного проверяющего абонента V в модифицированной схеме идентификации Штерна за T_B тактов. Машина состоит из двух частей, каждая из которых соответствует одному из шагов схемы.

$B(u,\sigma,y,b,\hat{b},s',M)$:
$(c_0,c_1,c_2,r_0',r_1',r_0'',r_1'') \longleftarrow B_1\,(u,\sigma,y,\hat{b},s',M)$,
$(r_0,r_1) \longleftarrow B_2\,(b,\hat{b},r_0',r_1',r_0'',r_1'')$.
Вернуть (c_0,c_1,c_2,r_0,r_1).

Определим теперь машины Тьюринга $\hat{A}$ и $\hat{B}$, использующие, помимо описанных стратегий, утечки по побочным каналам:

$\hat{A}(u,\sigma,y,b,\hat{b},T_1)$:
$s \leftarrow SC_1(T_1)$,
$(c_0,c_1,c_2,r_0,r_1) \leftarrow A(u,\sigma,y,b,\hat{b},s)$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

$\hat{B}(u,\sigma,y,b,\hat{b},T_1,T_2)$:
$(s',M) \leftarrow SC_2(T_1,T_2)$,
$(c_0,c_1,c_2,r_0,r_1) \leftarrow B(u,\sigma,y,b,\hat{b},s',M)$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

Обозначим за $T_{\hat{A}}$ и $T_{\hat{B}}$ время их работы в тактах.

Машины принимают на вход секретный ключ и маску, которые можно заменить случайными векторами при отсутствии физической возможности у противника выполнить атаку по побочным каналам, не нарушая общности.

Теорема 1: Время работы машин A и B совпадает.

Доказательство.

$A(u,\sigma,y,b,\hat{b},s) = B(u,\sigma,y,b,\hat{b},s,0)$,
$B(u,\sigma,y,b,\hat{b},s',M) = A(u \oplus M,\sigma,y,b,\hat{b},s' \oplus M)$.

Поскольку каждую из машин Тьюринга можно определить через другую, и считая дополнительные расходы в виде двух побитовых сложений пренебрежимо малыми, получаем

$$T_A = T_B.$$

Теорема 2: Время работы машины $\hat{A}$ меньше времени работы $\hat{B}$.

Доказательство. В силу определений заметим, что:

$$T_{\hat{A}} = T_{SC_1} + T_A,$$
$$T_{\hat{B}} = T_{SC_2} + T_B.$$

Используя теорему 1 и (7) получим

$$T_{\hat{A}} < T_{\hat{B}}.$$

Таким образом, без нарушения стойкости в модели без использования утечек по побочным каналам модификация схемы становится более устойчивой в модели с использованием утечек.

Заключение

Атаки по побочным каналам – серьёзная угроза безопасности не только классических криптографических схем, основанных на задачах теории чисел, но и постквантовых. Помимо аппаратной защиты устройств, стоит предусматривать и логическую, разрабатывая алгоритмы таким образом, чтобы потребляемое напряжение и излучаемые электромагнитные волны были максимально декоррелированы с секретными данными, над которыми проводятся вычисления.

Авторами был предложен вариант матричного умножения, повышающий стойкость схемы к этим атакам, и модификация схемы, позволяющая хранить и использовать приватный ключ в маскированном виде. Благодаря этому можно реализовывать схемы, основанные на протоколе идентификации Штерна, требующие от противника использовать более сложные и дорогостоящие методы атак.

Литература

1. Stern J. A new identification scheme based on syndrome decoding // Advances in Cryptology – CRYPTO' 93 / под ред. D. R. Stinson. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. – С. 13–21.
2. Fiat A., Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems // Advances in Cryptology – CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings. Т. 263. – Springer, 1986. – С. 186–194. – (Lecture Notes in Computer Science). – DOI: 10.1007/3-540-47721-7_12.
3. Vysotskaya, V. V. The security of the code-based signature scheme based on the Stern identification protocol / V. V. Vysotskaya, I. V. Chizhov // Applied Discrete Mathematics. – 2022. – No. 57. – P. 67–90. – DOI 10.17223/20710410/57/5.
4. Mano M. M., Ciletti M. D. Digital Design (4th Edition). – USA : Prentice-Hall, Inc., 2006. – С. 500–501.
5. Rabaey J. Digital Integrated Circuits: A Design Perspective. – Prentice Hall, 1996. – (Prentice Hall International editions).
6. Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model // Т. 3156. – 08.2004. – С. 16–29. – DOI: 10.1007/978-3-540-28632-5_2.
7. Kocher P. C., Jaffe J., Jun B. Differential Power Analysis // Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15–19, 1999, Proceedings. Т. 1666. – Springer, 1999. – С. 388–397. – (Lecture Notes in Computer Science). – DOI: 10.1007/3-540-48405-1_25.
8. Peeters E., Standaert F.-X., Quisquater J.-J. Power and electromagnetic analysis: Improved model, consequences and comparisons // Integration. – 2007. – Янв. – Т. 40. – С. 52–60. – DOI: 10.1016/j.vlsi.2005.12.013.
9. Laser attack benchmark suite / B. Amornpaisannon [и др.] // In: 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD). – 2020. – С. 1–9. – DOI: 10.1145/3400302.3415646.
10. Korkikian R., Pelissier S., Naccache D. Blind Fault Attack against SPN Ciphers // Proceedings - 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014. – 2014. – Дек. – С. 94—103. – DOI: 10.1109/FDTC.2014.19.
11. J. Breier and X. Hou Breier J., Hou X. How Practical Are Fault Injection Attacks, Really? // IEEE Access. – 2022. – Т. 10. – С. 113122–113130. – DOI: 10.1109/ACCESS.2022.3217212.
12. Lomné V., Roche T., Thillard A. On the Need of Randomness in Fault Attack Countermeasures - Application to AES //. – 09.2012. – С. 85–94. – DOI: 10.1109/FDTC.2012.19.
13. Reed-Solomon Codes for Satellite Communications / Y. Liu [и др.] // 2009 IITA International Conference on Control, Automation and Systems Engineering (case 2009). – 2009. – С. 246–249. – DOI: 10.1109/CASE.2009.30.
14. AlTawy R., Youssef A. M. Differential Fault Analysis of Streebog // Information Security Practice and Experience / под ред. J. Lopez, Y. Wu. – Cham : Springer International Publishing, 2015. – С. 35–49.

15. Horizontal Correlation Attack on Classic McEliece / B. Colombier [и др.]. – 2023. – Cryptology ePrint Archive, Paper 2023/546.
16. Prange E. The use of information sets in decoding cyclic codes // IRE Trans. Inf. Theory. – 1962. – Т. 8. – С. 5–9. – URL: https://api.semanticscholar.org/ CorpusID:3351723.
17. Towards Sound Approaches to Counteract Power-Analysis Attacks / S. Chari [и др.] // Annual International Cryptology Conference. – 1999. – URL: https://api.semanticscholar.org/CorpusID:16695847.
18. Rabas T., Buček J., Lorencz R. Single-Trace Side-Channel Attacks on NTRU Implementation // SN Computer Science. – 2024. – Т. 5. – DOI: 10.1007/s42979-023-02493-7.
19. Prouff E., Rivain M. Masking against Side-Channel Attacks: A Formal Security Proof // Advances in Cryptology – EUROCRYPT 2013 / под ред. T. Johansson, P.Q. Nguyen. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. – С. 142–159.
20. L.R. Akhmetzyanova, A.A. Babueva, A.A.B. Streebog as a random oracle // ПДМ. – 2024. – № 64. – С. 27–42. – DOI: 10.17223/20710410/64/3.
21. Rosulek M. The Joy of Cryptography // – 2017. – URL: https://api.semanticscholar.org/CorpusID:199008788.
22. Cayrel P.-L., Gaborit P., Prouff E. Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices // Smart Card Research and Advanced Applications / под ред. G. Grimaud, F.-X. Standaert. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008. – С. 191–205. – DOI: 10.1007/978-3-540-85893-5_14.

METHODS OF PROTECTION AGAINST SIDE-CHANNEL ATTACKS IN THE HARDWARE IMPLEMENTATION OF POST-QUANTUM SIGNATURE SCHEMES BASED ON THE STERN IDENTIFICATION PROTOCOL

Smirnov D.K.[3], Chizhov I.V.[4]

Keywords: *syndrome decoding, «Shipovnik» signature scheme, correlation attack, electromagnetic radiation attack, energy consumption attack, fault injection attack.*

Purpose of the study: *the development of a secure Stern identification protocol resistant to side-channel attacks.*

Methods of research: *the study of modern techniques for attacking cryptographic systems with similar computational components, methods to protect against these attacks, and modifications to the system in order to safeguard the private key in the event of a token theft.*

Result(s): *Vulnerable computational elements of the protocol, such as addition of vectors modulo 2 and matrix multiplication by a vector, are identified. The main methods of protecting these elements from leakage through side channels, including masking, balancing, and mixing, are analyzed. A matrix multiplication method resistant to horizontal correlation attacks used against the McEliece cryptosystem is proposed. The basic requirements for implementing the scheme on field-programmable gate arrays (FPGAs) are established. A modification of the scheme with key masking that does not compromise the strength of the original scheme is proposed to protect the secret in the event of token theft and prevent impersonation attacks due to key masking. The method of key mask generation is selected to minimize the amount of space occupied on an FPGA, specifically by hashing the passphrase using the «Stribog-K» function with a counter. It has been shown that the stability of the modified Stern identification protocol is the same as the stability of the original protocol in a model without side channel leakage, and it is even better in a model with side channel leakage.*

Scientific novelty: *the results of the work allow us to implement the post-quantum signature algorithm «Shipovnik», which is being developed by the TK26 working group and is currently being standardized.*

References

1. Stern, J. (1994). A New Identification Scheme Based on Syndrome Decoding. Advances in Cryptology – CRYPTO' 93, 773, 13–21. https://doi.org/10.1007/3-540-48329-2_2.
2. Fiat, A., & Shamir, A. (1986). How To Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology — CRYPTO' 86, 263, 186–194. https://doi.org/10.1007/3-540-47721-7_12.
3. Vysotskaya, V., Chizhov, I. (2022). The security of the code-based signature scheme based on the Stern identification protocol. Prikladnaya diskretnaya matematika, (57), 67–90. https://doi.org/10.17223/20710410/57/5.
4. Mano M.M., Ciletti M.D. (2006). Digital Design (4th ed.). Prentice-Hall, Inc.
5. Rabaey, J.M., Chandrakasan, A.P., & Nikolić, B. (2003). Digital Integrated Circuits: A Design Perspective (2nd ed.). Pearson Education.
6. Brier, E., Clavier, C., Olivier, F. (2004). Correlation Power Analysis with a Leakage Model. Cryptographic Hardware and Embedded Systems – CHES 2004, 3156. https://doi.org/10.1007/978-3-540-28632-5_2.
7. Kocher, P., Jaffe, J., Jun, B. (1999). Differential Power Analysis. Advances in Cryptology – CRYPTO' 99, 1666. https://doi.org/10.1007/3-540-48405-1_25.

3 Dmitrii K. Smirnov, master, Lomonosov Moscow State University, Moscow, Russia. E-mail: s02190708@stud.cs.msu.ru
4 Ivan V. Chizhov, Ph.D., Lomonosov Moscow State University, Federal Research Center «Informatics and Control» of Russian Academy of Science, JSC «NPK Kryptonite», Moscow, Russia. E-mail: ichizhov@cs.msu.ru

8. Peeters E., Standaert F.-X., Quisquater J.-J. (2007). Power and electromagnetic analysis: Improved model, consequences and comparisons. Integration, 40, 52-60. https://doi.org/10.1016/j.vlsi.2005.12.013.
9. Amornpaisannon, B., Diavastos, A., Peh, L., & Carlson, T. E. (2020). Laser Attack Benchmark Suite. Proceedings of the 39th International Conference on Computer-Aided Design, 1–9. https://doi.org/10.1145/3400302.3415646.
10. Korkikian, R., Pelissier, S., & Naccache, D. (2014). Blind Fault Attack against SPN Ciphers. 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, 94–103. https://doi.org/10.1109/FDTC.2014.19.
11. Breier, J., & Hou, X. (2022). How Practical Are Fault Injection Attacks, Really? IEEE Access, 10, 113122–113130. https://doi.org/10.1109/ACCESS.2022.3217212.
12. Lomné, V., Roche, T., & Thillard, A. (2012). On the Need of Randomness in Fault Attack Countermeasures – Application to AES. 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, 85–94. https://doi.org/10.1109/FDTC.2012.19.
13. Liu, Y., Guan, Y., Zhang, J., Wang, G., & Zhang, Y. (2009). Reed-Solomon Codes for Satellite Communications. 2009 IITA International Conference on Control, Automation and Systems Engineering (Case 2009), 246–249. https://doi.org/10.1109/CASE.2009.30.
14. AlTawy, R., Youssef, A.M. (2015). Differential Fault Analysis of Streebog. Information Security Practice and Experience, 9065. https://doi.org/10.1007/978-3-319-17533-1_3.
15. Colombier, B., Grosso, V., Cayrel, P., & Drăgoi, V. (2023). Horizontal Correlation Attack on Classic McEliece. https://eprint.iacr.org/2023/546.
16. Prange, E. (1962). The Use of Information Sets in Decoding Cyclic Codes. IRE Transactions on Information Theory, 8(5), 5–9. https://doi.org/10.1109/TIT.1962.1057777.
17. Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P. (1999). Towards Sound Approaches to Counteract Power-Analysis Attacks. Advances in Cryptology – CRYPTO' 99, 1666. https://doi.org/10.1007/3-540-48405-1_26.
18. Rabas, T., Buček, J., & Lórencz, R. (2024). Single-Trace Side-Channel Attacks on NTRU Implementation. SN Computer Science, 5(2), 239. https://doi.org/10.1007/s42979-023-02493-7.
19. Prouff, E., Rivain, M. (2013). Masking against Side-Channel Attacks: A Formal Security Proof. Advances in Cryptology – EUROCRYPT 2013, 7881. https://doi.org/10.1007/978-3-642-38348-9_9.
20. Akhmetzyanova, L.R., Babueva, A.A., & Bozhko, A.A. (2024). Streebog as a Random Oracle. PDM, 64, 27–42. https://doi.org/10.17223/20710410/64/3.
21. Rosulek, M. (2017). The Joy of Cryptography.
22. Cayrel, P.L., Gaborit, P., Prouff, E. (2008). Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices. Smart Card Research and Advanced Applications, 5189. https://doi.org/10.1007/978-3-540-85893-5_14.