КВАНТОВО-УСИЛЕННЫЙ СИММЕТРИЧНЫЙ КРИПТОАНАЛИЗ S-AES

Моисеевский А.Д.[1], Манько С.Д.[2]

DOI: 10.21681/2311-3456-2025-3-55-62

Цель исследования: *исследование возможности снижения ресурсных требований к реализации атаки алгоритмом Гровера на блочные шифры на примере упрощённого шифра S-AES. Исследование возможностей учёта частичной утечки ключа. Оценка необходимых ресурсов и численное моделирование квантовой атаки на S-AES со сниженными требованиями.*

Методы исследования: *алгебраический анализ, численное моделирование.*

Результаты исследования: *продемонстрирована возможность существенного снижения числа кубитов за счёт оптимизации оракула при реализации атаки алгоритмом Гровера на симметричные блочные шифры на примере S-AES. Необходимые для моделирования квантовой атаки S-AES ресурсы снижены достаточно, чтобы стало возможным исследование данного алгоритма посредством численного моделирования на ПК с 400Мб ОЗУ за время порядка 30 минут (в зависимости от конфигурации CPU). Благодаря этому проведено численное моделирование квантовой атаки на S-AES для идеального случая и с учётом элементарных шумов квантового вычислителя.*

Научная новизна: *предложен новый алгоритм квантовой атаки на шифр S-AES с существенно сниженными требованиями по числу кубитов. Проведено численное моделирование атаки при помощи данного алгоритма, что для известных ранее атак было практически невозможно. Результаты иллюстрируют, что наши представления о ресурсных требованиях квантовой атаки и, как следствие, возможном горизонте её практической реализации могут быть существенно ошибочными, если будет найден альтернативный способ реализации даже уже известного концептуально и асимптотически не улучшаемого алгоритма квантовой атаки.*

Ключевые слова: *квантовые вычисления, квантовый криптоанализ, квантовая угроза, симметричное шифрование, S-AES.*

Введение

Наравне с алгоритмом Шора, алгоритм Гровера уже более 20 лет рассматривается как актуальная угроза информационной безопасности [1]. Для симметричных шифров именно асимптотическую устойчивость к атаке Гровера Национальный Институт Стандартов и Технологий (NIST) принимает за меру пост-квантовой стойкости криптографического алгоритма [2]. Данная атака позволяет корневым образом сокращать асимптотическую сложность перебора симметричного ключа. Следовательно, для сохранения прежней криптографической стойкости и ожидаемого времени конфиденциальности зашифрованных данных, возникает необходимость использовать в два раза более длинные ключи. Такая угроза не является критической для информационной безопасности в целом, однако может требовать внимания в случае перехвата сообщений, зашифрованных по не учитывающему данную угрозу стандарту. Оценка связанных с этим рисков требует понимания того, какими характеристиками должен обладать квантовый компьютер для реализации подобной атаки.

Реализации подобной угрозы препятствуют в основном два сдерживающих фактора: доступный размер регистра квантового вычислителя и ограниченное количество операций, которые можно произвести с кубитом за время его когерентности. Таким образом главным параметром шифра при оценке его подверженности квантовой атаке является длина ключа, которая определяет необходимое число кубитов для реализации алгоритма. При этом ограничение, связанное с конечным временем когерентности кубита и предельным количеством операций в алгоритме, хоть и также является крайне существенным, не настолько критично, поскольку влияние шумов, в отличие от числа кубитов, в большинстве случаев может быть уменьшено минимальным вмешательством в конструкцию аппаратной установки и использованием методов подавления ошибки [3]. Недостаток же числа кубитов на имеющимся аппаратном обеспечении является строгим ограничением, и может быть исправлен только существенной переработкой экспериментальной установки. Исключением, с некоторыми техническими оговорками, можно назвать архитектуру квантовых вычислителей на основе холодных атомов.

Количество кубитов, необходимых для атаки как симметричных, так и асимметричных шифров, в первую очередь определяется размером используемого

1 Моисеевский Алексей Денисович, АО «ИнфоТеКС», ООО «С-Квантум», Центр Квантовых Технологий МГУ им. М.В. Ломоносова. Москва, Россия. E-mail: Aleksey.Moiseevsky@infotecs.ru

2 Манько Софья Дмитриевна, АО «ИнфоТеКС». Москва, Россия. E-mail: Sofia.Manko@infotecs.ru

ключа. При этом длина ключа в симметричном стандарте AES составляет от 128 до 256 бит [4]. С 2011 г. существует также версия AES-512, однако данная версия не принята в настоящее время в качестве стандарта [5]. Рекомендуемая же длина ключа для асимметричного стандарта RSA составляет от 2048 бит [6]. Если не принимать во внимание работу [7], подвергнутую всесторонней критике [8, 9], то длину ключа можно рассматривать как неточную оценку снизу для объёма квантового регистра, необходимого для атаки. Крупнейшие на момент начала 2025 года квантовые вычислители обладают регистром в 1225 [10] и 1180 [11] физических кубитов, подверженных влиянию шумов. Таким образом сегодня не существует квантовых вычислителей, способных осуществлять полную атаку на какие-либо принятые стандарты шифрования. Но можно ожидать, что экспериментальная реализация квантовой атаки на шифры с закрытым ключом станет возможна значительно раньше, чем на методы асимметричной криптографии.

Предыдущие и новые результаты

Исследование аспектов практической реализации атаки алгоритмом Гровера на AES 128 было проведено в работе [12]. Представленные результаты позволяют реализовывать атаку Гровера на шифр AES-128 с использованием 264 кубитов. Поскольку асимптотически атака Гровера не может быть улучшена, интерес представляет исследование возможности ещё большего снижения данного значения, например за счёт частичной утечки ключа вследствие атаки по побочному каналу.

Поскольку моделирование 264-кубитного регистра находится далеко за рамками возможностей классических симуляторов квантового компьютера, первоначальное исследование было проведено для упрощённого шифра S-AES [13]. S-AES представляет собой блочный шифр с 16-битным ключом, 16-битным текстом и двумя раундами. Прямая атака Гровера на S-AES требует 32-кубитного регистра и принципиально может быть промоделирована с помощью классического симулятора, хотя данная процедура и потребует больших вычислительных ресурсов. Это открывает возможности для исследования концепций оптимизации атаки на примере данного упрощённого шифра. Всесторонний анализ вопросов реализации атаки алгоритмом Гровера на S-AES, включая построение квантовых вариантов преобразований S-Box и MixColumn проведён в работах [14, 15].

В данной работе описывается концепция квантовой атаки на S-AES с частичной утечкой ключа и идея общей оптимизации оракула. Оригинальная оптимизированная атака, названная в дальнейшем атакой разделением, позволяет производить ускоренный поиск ключа с использованием $23 - 4n$ кубитов, где $n \in [1;3]$ – число известных полубайтов ключа. Снижение требований для объёма квантового регистра до 23 кубитов в общем случае позволило моделировать квантовую атаку на ПК и с использованием графических ускорителей. Это, в свою очередь, позволило произвести оценку шумовой устойчивости квантового алгоритма к элементарным ошибкам.

Сравнительные данные по промоделированным в работе методам атаки, а также сравнение с прямой атакой на S-AES, описанной в [14], приведены в таблице 1. Приводятся результаты для обычной 32-кубитной атаки, атаки с утечкой первого байта ключа, атаки разделением и атаки разделением с утечкой одного байта ключа. Приводимые характеристики – число кубитов, необходимое для атаки, глубина схемы (число слоёв при максимальной параллелизации применения гейтов), общее число запутывающих двухкубитных гейтов CNOT, время симуляции на ПК с 8-ядерным ЦП 2,5 ГГц и 64 Гб RAM. Моделирование атаки разделением без утечки использует 400 Мб RAM. Моделирование прямой 32-кубитной атаки на ПК с данными характеристиками невозможно. Разброс в значении глубины схемы объясняется необходимостью многократной загрузки открытого текста и шифртекста в квантовый регистр в ходе итераций Гровера, что осуществляется с помощью классически-контролируемых гейтов, число которых определяется конкретным битовым представлением текста.

Таблица 1.

Соотношение ресурсов, необходимых для реализации и моделирования атаки Гровера на S-AES с различным типом оракула

Оракул	Число кубитов	Глубина	Число CNOT	$t_{симуляции}$
Обычный [14]	32	459 512 ± 100	478 380	–
С утечкой второго байта ключа	24	24 191 ± 9	19 092	60 с
Разделением	23	1 698 762 ± 1289	2 195 724	1080 с
Разделением, с утечкой одного байта ключа	15	73 678 ± 99	58 944	5 с

Прямая атака Гровера на S-AES

Изначально алгоритм Гровера является ускоренным алгоритмом поиска по неструктурированной базе данных [1]. Если для искомого элемента базы данных выполняется уравнение $f(x) = 1$, а для остальных $f(x) = 0$, и реализовано квантовое преобразование

$$\hat{U}|x\rangle = (-1)^{f(x)}|x\rangle, \quad (1)$$

алгоритм Гровера позволяет найти искомый элемент за число обращений к оператору $\hat{U}$, равное

$$R = \lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \rfloor. \quad (2)$$

Здесь N – общее число элементов базы данных, M – число элементов, удовлетворяющих уравнению $f(x) = 1$. В случае поиска по множеству n-битных ключей, $N = 2n$. Оператор $\hat{U}$ называется оракулом и является подпрограммой алгоритма Гровера. При этом оракул содержит всю информацию о решаемой задаче, остальной алгоритм в зависимости от конкретной поставленной задачи не меняется.

Выражение (1) означает, что оператор $\hat{U}$ должен инвертировать фазу состояния $|x\rangle$, соответствующего искомому элементу, и оставлять неизменными все остальные состояния [16]. Это позволяет получить ясное представление об устройстве оракула, делающего алгоритм Гровера полезным в приложении задач криптоанализа.

Рассматривается задача атаки открытого текста: для заданного открытого текста и шифртекста необходимо определить ключ, которым было произведено зашифрование. Решение подобной задачи представляет интерес с практической точки зрения, поскольку тот же ключ мог быть использован для шифрования других данных. Утверждается, что не существует иного способа отыскания ключа по тексту и шифртексту, кроме перебора. Для ускорения перебора может быть использован алгоритм Гровера.

В результате выполнения алгоритма состояние $|x\rangle$ должно содержать единственную доминирующую амплитуду, индекс которой в битовом представлении соответствует предполагаемому ключу. Оракул $\hat{U}$ может содержать информацию о текстах, в том числе в дополнительных кубитах. Функцией $\hat{U}$ для задачи криптоанализа будет зашифрование открытого текста с помощью ключа $|x\rangle$ и сравнение результата с известным шифртекстом. Если полученный и заданный шифртексты совпадают, оператор $\hat{U}$ должен инвертировать фазу состояния $|x\rangle$. Блок PTXT обозначает инициализацию квантового регистра данными классического текста через классически-контролируемые гейты $\hat{X}$. Сравнение текстов может быть произведено путём добавления в квантовый регистр классических данных о зашифрованном тексте. На рис. 1 данная операция показана блоком !CTXT. Если бит шифртекста с некоторым индексом равен 0, то операция !CTXT подействует оператором $\hat{X}$ на кубит с тем же индексом. Таким образом, если на вход оракула подавался корректный ключ, после действия операции !CTXT все дополнительные кубиты (не кубиты текста) будут находиться в состоянии $|1\rangle$, и действующий на них оператор C16Z инвертирует фазу данного состояния (Здесь и далее как CnZ или CnNOT обозначаются условные операторы, контролируемые несколькими кубитами: C1Z – CZ, C1NOT – CNOT, C2NOT – оператор Тоффоли и т.д.). Дальнейшие обратные преобразования в оракуле приведут дополнительные кубиты к состоянию $|0\rangle$, а кубиты ключа – к состоянию $U|x\rangle$. Оракул для атаки AES-128 может быть построен аналогичным образом с точностью до числа кубитов и раундов.

Прямая атака S-AES с утечкой

Описанная выше атака требует 32 кубита. Симуляция алгоритма с регистром такого объёма даже при эмуляции идеальной унитарной динамики чистых состояний требует более 40 ГБ оперативной памяти, что делает практически невозможным симуляцию данной атаки на GPU. Возможный способ уменьшить количество требуемых кубитов — рассмотреть случай, когда часть битов ключа оказывается известна благодаря атаке по стороннему каналу.

Как можно видеть на рис. 1, в спецификации S-AES 16-битные ключи раунда делятся на два

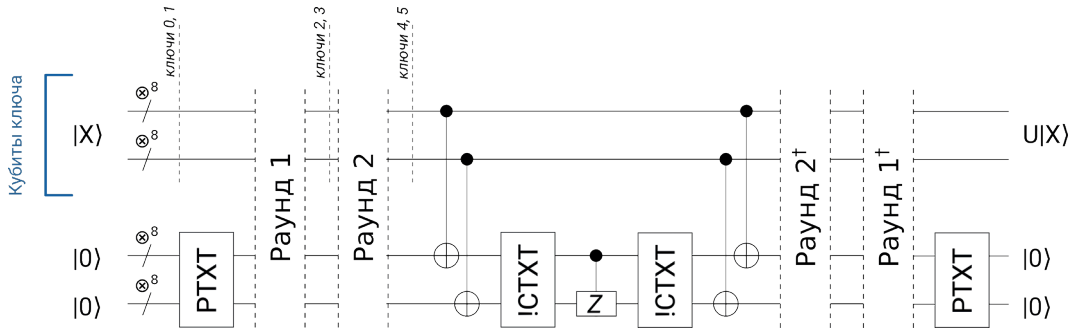

Рис. 1. Топологическая схема оракула для прямой 32-кубитной атаки Гровера на S-AES. AES может быть построен аналогичным образом с точностью до числа кубитов и раундов.

8-битных сегмента, обычно обозначаемых B. Текст делится на два 8-битных сегмента, обозначаемых $N_{1,2}$. Рассмотрим простой случай, когда ключ B_1 оказался известен. Для этого, во-первых, определим алгебраические выражения ключей раундов. Исходные ключи обозначаются как B_0 и B_1, ключи первого раунда – B_2 и B_3, второго – B_4 и B_5. Здесь и далее обозначение операций побитового сложения опускаются для краткости.

$$B_0 = B_0 \qquad B_3 = B_1B_2 = C_0B_0B_1B_1^{SR}$$
$$B_1 = B_1 \qquad B_4 = C_1B_2B_3^{SR} = C_0C_1B_0B_1^{SR}[C_0B_0B_1B_1^{SR}]^{SR} \quad (3)$$
$$B_2 = C_0B_0B_1^{SR} \qquad B_5 = B_3B_4 = C_1B_1B_2B_2B_3^{SR} = C_1B_1B_3^{SR}$$

Здесь C_0 и C_1 — специфицированные константы раундов, верхние индексы S и R обозначают действие операций подстановки (S-Box) и разворота полубайтов (RotateNibble). Интерес представляет вопрос, можно ли использовать дополнительные данные о битах ключа для модификации алгоритма и распутывания (факторизации) кубитов, соответствующих известным битам от состояния остального квантового регистра.

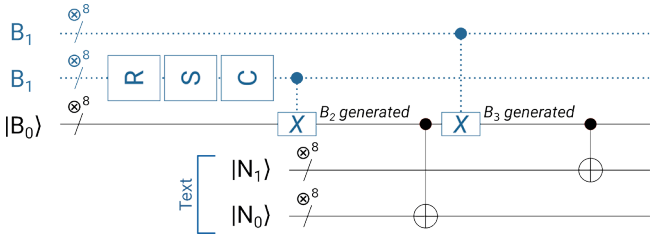

Рис. 2. Расширение ключа при частном случае утечки.

Блоки R, S и C обозначают операции RotateNibble, S-Box и AddConst соответственно.

На рис. 2 показан процесс расширения ключа при утечке исходного байта B_1. Данные B_1 находятся в классической памяти, что обозначено цветным пунктиром. Не представляет сложности генерация B_2 в кубитах, в которых исходно хранился байт B_0. Генерация B_3 затем может быть произведена после использования B_2, в тех же кубитах, с использованием классической копии B_1.

Определённую сложность представляет генерация B_4. Как видно из формул (3), выражение B_4 включает в себя битовую сумму B_0 со значением функции S-Box, аргумент которой также содержит B_0. Таким образом, данное выражение становится необратимым, процедура его генерации становится неунитарным преобразованием, соответственно, не может быть реализована в виде квантовой программы без привлечения дополнительных кубитов.

Обойти данную проблему можно путём перехода от генерации B_4 сразу к вычислению результатов раунда для регистра текста, добавляя слагаемые B_4 к тексту последовательно, как это показано на рис. 3.

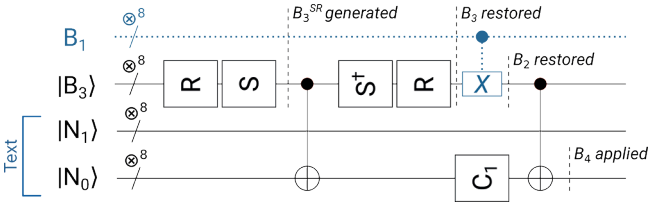

Рис. 3. Добавление ключа раунда B_4 к байту текста N_0 без непосредственного расчёта B_4 в кубитах регистра.

Генерация B_5 также не представляет сложностей и является обратимой. Таким образом при утечке B_1 возможна реализация атаки всего на 24 кубитах вместо 32, что уже доступно для численного моделирования на GPU. Однако описанный подход оказывается невозможен при утечке B_0. По этой причине для построения общей оптимизированной атаки требуется иной подход.

Атака S-AES разделением

В основе атаки разделением лежит идея повторного использования кубитов за счёт последовательной генерации полубайтов текста. Вместо хранения полного текста и полного ключа в 32 кубитах, выделяется 16 кубитов на работу с ключом и 4 кубита для работы с текстом. В регистре ключа происходит процедура генерации ключей раунда, в то время как в регистре текста генерируется зашифрованный полубайт. Далее происходит сравнение полученного полубайта с соответствующим полубайтом известного шифртекста. Результат записывается в 1 кубит-анциллу с помощью гейта C4NOT с четырьмя контрольными и одним целевым кубитом. Повторив данную процедуру для трёх полубайтов 16-битного текста, сохранив результаты сравнения в три кубита-анциллы и проведя сравнение для последнего полубайта в 4 кубитах регистра текста, необходимо подействовать на регистр текста и анциллы гейтом C7Z. В случае, если на вход оракула был подан корректный ключ, значение всех анцилл, а также кубитов регистра текста будет $|1\rangle$, и гейт C7Z инвертирует фазу данного состояния. Данные шаги изображены на рис. 4. Далее, аналогично схеме на рис. 1 необходимо произвести обратные преобразования для восстановления исходных значений кубитов в регистре ключа.

В общем случае для атаки разделением требуется 23 кубита. Верхний индекс операции !CTXT указывает, какой полубайт шифртекста сравнивается с содержимым регистра. Преобразование $Round\ A.B$ на рис. 4 генерирует один из четырёх полубайтов результата раунда. A обозначает номер раунда, а B обозначает номер полубайта результата.

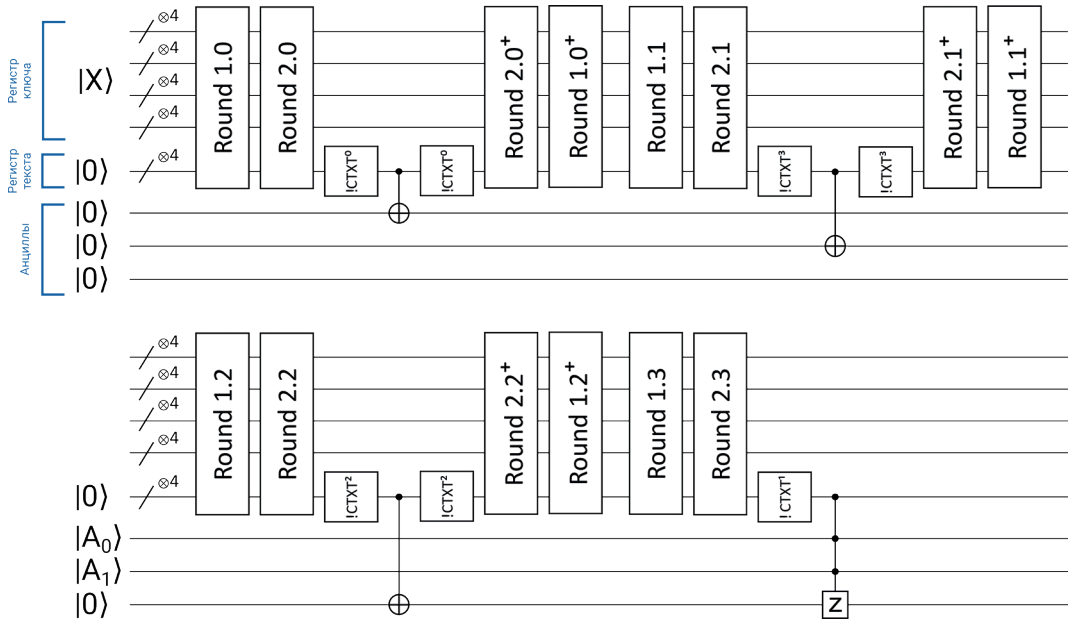

Рис. 4. Топологическая схема оракула атаки разделением.

Данная конфигурация оракула требует $N = 16$ (регистр ключа) + 4 (регистр текста) + 3 (анциллы) = = 23 кубита. Также данная атака естественным образом обрабатывает любую полубайтовую утечку, обеспечивая соответствующую дополнительную экономию кубитов.

Ключевым элементом при обработке утечки, а также в целом при пополубайной генерации шифтекста

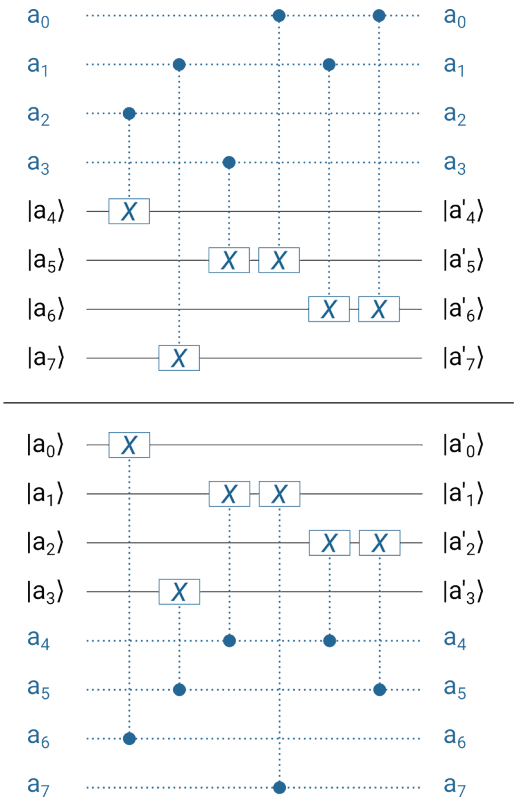

Рис. 5. Схемы гибридного преобразования MixColumn.

является схема частичного преобразования MixColumn (далее MC). Преобразование MC является одним из базовых в шифрах AES и S-AES, и применяется в ходе раунда. В случае S-AES оно действует на 8 битов и генерирует 8-битный результат. Поскольку для каждого байта результирующего шифртекста требуется сгенерировать сначала первый полубайт, а затем второй, необходимо сконструировать 8-кубитное преобразование, которое сохраняет состояние одного входного полубайта неизменным, а во втором способно генерировать как первый, так и второй полубайт результата. Для обеспечения возможности обработки утечки также необходимо избежать использования запутывающих гейтов CNOT, для которых кубиты, оставляемые в преобразовании неизменными, являлись бы целевыми. Схемы данных преобразований следуют из спецификации S-AES и представлены на рис. 5.

Преобразование действует на 8 кубитов, из которых 4 остаются неизменными, а на месте оставшихся четырёх генерируется один из двух полубайтов результата обычного преобразования MixColumns. Кубиты, которые остаются неизменными, обозначены на рис.5 цветным пунктиром. Поскольку данные кубиты выступают исключительно контрольными, в случае частичной утечки вместо них могут быть использованы классические биты. Данных преобразований достаточно для реализации атаки разделением с любой конфигурацией полубайтов утечки.

Моделирование оптимизированной атаки S-AES

В ходе работы было проведено моделирование полной атаки разделением, атаки разделением с утечкой и прямой атаки с утечкой B_1. Ресурсные

характеристики квантовых схем данных атак представлены в таблице 1.

Снижение ресурсных требований к моделированию на классических симуляторах позволило произвести анализ устойчивости атак к элементарным квантовым шумам: ошибке инвертирования значения бита (вероятностное применение оператора $\hat{X}$) и инвертирования фазы (вероятностное применение оператора $\hat{Z}$) при применении двухкубитного гейта в декомпозированной схеме. Полученные в результате зависимости вероятности определения корректного ключа от вероятности ошибки представлены на рис. 6 и рис. 7.

Получение подобных зависимостей без привлечения алгоритмов атаки с утечкой и атаки разделением было практически нереализуемо, поскольку однократное исполнение полной 32-кубитной атаки Гровера на S-AES с шумовой моделью на вычислительном кластере Центра квантовых технологий МГУ занимало более 480 часов. На представленных же графиках каждая точка получена усреднением по 50 запускам.

Данные графики позволяют сформировать представление о величине шумов, которым может быть подвержен квантовый компьютер для практического применения в задачах квантового криптоанализа. Очевидно, что влияние шумов на алгоритм атаки на полноценные шифры AES-128 и AES-256 будет ещё на порядок выше. При этом из графиков можно сделать вывод, что атака разделением более чувствительна к шумовому воздействию, очевидно, за счёт значительно большей глубины алгоритма. Однако необходимо помнить, что данная атака требует меньше кубитов, а при условно сопоставимом техническом исполнении аппаратного обеспечения, уровень ошибок в регистре меньшего объёма будет ниже. Убедиться в этом можно на примере дорожной карты квантовых вычислителей IBM [11]. Анализ возможности расширения представленных концепций экономии кубитов для AES-128 и построение подобных графиков шумовой устойчивости хотя бы для исключительных случаев с утечкой большей части ключа позволит расширить понимание подходов к перспективной задаче квантового криптоанализа и обеспечить большую степень готовности к реализации квантового превосходства для отрасли информационной безопасности.

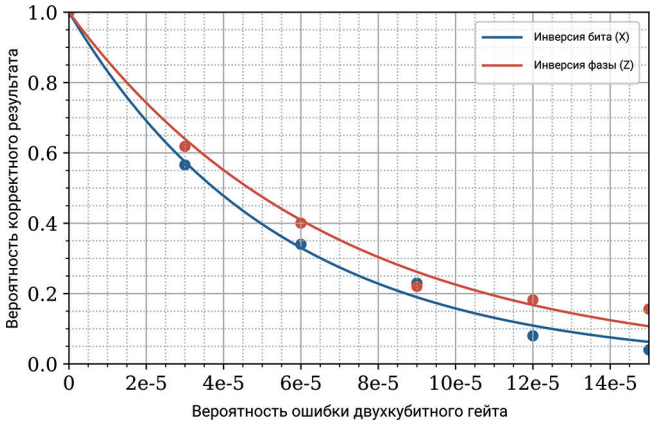

Рис. 6. Зависимость вероятности обнаружения корректного ключа от вероятности битовой и фазовой ошибки двухкубитного гейта для прямой атаки с утечкой (24 кубита). Аппроксимация $y = e^{-ax}$, Для ошибки фазы a = 18468, для ошибки бита a = 14893

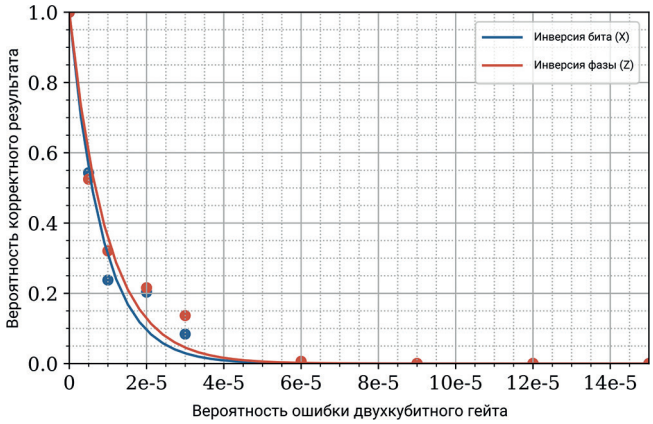

Рис. 7. Зависимость вероятности обнаружения корректного ключа от вероятности битовой и фазовой ошибки двухкубитного гейта для разделением атаки с утечкой (15 кубитов). Аппроксимация $y = e^{-ax}$. Для ошибки фазы a = 117545, для ошибки бита a = 102862

Литература

1. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing. – 1996. – С. 212–219.
2. NIST. FAQ on Kyber512 // URL: csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/Kyber-512-FAQ.pdf. – 2023.
3. Cai Z. et al. Quantum error mitigation //Reviews of Modern Physics. – 2023. – Т. 95. – №. 4. – С. 045005. DOI: 10.1103/RevModPhys.95.045005.
4. NIST. Advanced Encryption Standard (AES) // Federal Information Processing Standards Publication 197. - 2001. DOI: 10.6028/NIST.FIPS.197.
5. Moh'd A., Jararweh Y., Tawalbeh L. AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. || In Information Assurance and Security (IAS) //2011 7th International Conference on. – С. 292–297. DOI: 10.1109/ISIAS.2011.6122835.
6. Ferraiolo H., Regenscheid A. Cryptographic algorithms and key sizes for personal identity verification // National Institute of Standards and Technology Special Publication 800. – 2024. DOI: 10.6028/NIST.SP.800-78-5.
7. Yan B. et al. Factoring integers with sublinear resources on a superconducting quantum processor //arXiv preprint arXiv:2212.12372. – 2022.

8. Khattar T., Yosri N. A comment on «Factoring integers with sublinear resources on a superconducting quantum processor» // arXiv preprint arXiv:2307.09651. – 2023.
9. Grebnev S. V. et al. Pitfalls of the sublinear QAOA-based factorization algorithm // IEEE Access. – 2023. – Т. 11. – С. 134760–134768. DOI: 10.1109/ACCESS.2023.3336989.
10. Atom Computing. Quantum startup Atom Computing first to exceed 1,000 qubits // URL: https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/. – 2023.
11. IBM. IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility // URL: newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility. – 2023.
12. Li Z. et al. New record in the number of qubits for a quantum implementation of AES //Frontiers in Physics. – 2023. – Т. 11. – С. 1171753. DOI: 10.3389/fphy.2023.1171753.
13. Musa M. A., Schaefer E. F., Wedig S. A simplified AES algorithm and its linear and differential cryptanalyses // Cryptologia. – 2003. – Т. 27. – №. 2. – С. 148–177. DOI: 10.1080/0161-110391891838.
14. Jang K. B. et al. Grover on simplified aes //2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). – IEEE, 2021. – С. 1–4. DOI: 10.1109/ICCE-Asia53811.2021.9642017.
15. Almazrooie M. et al. Quantum Grover attack on the simplified-AES //Proceedings of the 2018 7th International Conference on Software and Computer Applications. – 2018. – С. 204–211. DOI: 10.1145/3185089.3185122.
16. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Перевод с английского под редакцией М. Н. Вялого и П. М. Островского с предисловием К. А. Валиева // Москва «МИР». – 2006. С. 311–320.

QUANTUM-ENHANCED SYMMETRICAL CRYPTOANALYSIS OF S-AES

Moiseevskiy A. D.[3], Manko S. D.[4]

Keywords: *quantum computing, quantum cryptanalysis, quantum threat, symmetric encryption, S-AES.*

Objective of the study: *to study the possibility of reducing quantum resource requirements for Grover's algorithm attack on block ciphers. Simplified-AES is considered as an example. To investigate the possibilities of using a partial key leakage. To estimate the required resources and to simulate a quantum attack on S-AES with reduced requirements.*

Research methods: *algebraic analysis, numerical simulation.*

Research results: *we have demonstrated the possibility of significantly reducing the number of qubits required to attack Simplified-AES by optimizing Grover's oracle. The resource requirements are reduced sufficiently, allowing to study quantum attack on Simplified-AES using numerical simulation on a PC with 400 MB of RAM in about 30 minutes (depending on the CPU configuration). A numerical simulation of a quantum attack on S-AES has been carried out for the case of an ideal leakage configuration, taking into account the elementary quantum noises.*

Scientific novelty: *a new quantum attack algorithm for Simplified-AES cipher with significantly reduced requirements for the qubits number is proposed. Numerical simulation of the attack using this algorithm is carried out, which was practically impossible for previously known approaches. The results illustrate that our ideas about the resource requirements for a quantum attack and, as a consequence, the possible time of its practical implementation can be significantly incorrect if an alternative method for implementing even an already known asymptotically unimprovable quantum attack algorithm is found.*

References

1. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. – 1996. – S. 212–219.
2. NIST. FAQ on Kyber512 //URL: csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/Kyber-512-FAQ.pdf. – 2023.
3. Cai Z. et al. Quantum error mitigation // Reviews of Modern Physics. – 2023. – Т. 95. – №. 4. – S. 045005. DOI: 10.1103/RevModPhys.95.045005.
4. NIST. Advanced Encryption Standard (AES) // Federal Information Processing Standards Publication 197. - 2001. DOI: 10.6028/NIST.FIPS.197.
5. Moh'd A., Jararweh Y., Tawalbeh L. AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. || In Information Assurance and Security (IAS) //2011 7th International Conference on. – S. 292–297. DOI: 10.1109/ISIAS.2011.6122835.
6. Ferraiolo H., Regenscheid A. Cryptographic algorithms and key sizes for personal identity verification //National Institute of Standards and Technology Special Publication 800. – 2024. DOI: 10.6028/NIST.SP.800-78-5.
7. Yan B. et al. Factoring integers with sublinear resources on a superconducting quantum processor //arXiv preprint arXiv:2212.12372. – 2022.

3 Alexey D. Moiseevskiy, InfoTeCS JSC, S-Quantum LLC, MSU Quantum Technology Centre. Moscow, Russia. E-mail: Aleksey.Moiseevsky@infotecs.ru
4 Sofya D. Manko, InfoTeCS JSC. Moscow, Russia. E-mail: Sofia.Manko@infotecs.ru

8. Khattar T., Yosri N. A comment on «Factoring integers with sublinear resources on a superconducting quantum processor» //arXiv preprint arXiv:2307.09651. – 2023.
9. Grebnev S.V. et al. Pitfalls of the sublinear QAOA-based factorization algorithm // IEEE Access. – 2023. – T. 11. – S. 134760-134768. DOI: 10.1109/ACCESS.2023.3336989.
10. Atom Computing. Quantum startup Atom Computing first to exceed 1,000 qubits // URL: https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/. – 2023.
11. IBM. IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility // URL: newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility. – 2023.
12. Li Z. et al. New record in the number of qubits for a quantum implementation of AES //Frontiers in Physics. – 2023. – T. 11. – S. 1171753. DOI: 10.3389/fphy.2023.1171753.
13. Musa M.A., Schaefer E.F., Wedig S. A simplified AES algorithm and its linear and differential cryptanalyses // Cryptologia. – 2003. – T. 27. – №. 2. – S. 148–177. DOI:10.1080/0161-110391891838.
14. Jang K.B. et al. Grover on simplified AES // 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). – IEEE, 2021. – S. 1–4. DOI: 10.1109/ICCE-Asia53811.2021.9642017.
15. Almazrooie M. et al. Quantum Grover Attack on the Simplified-AES // Proceedings of the 2018 7th International Conference on Software and Computer Applications. – 2018. – S. 204–211. DOI: 10.1145/3185089.3185122.
16. Nielsen M., Chuang I. Quantum Computation and Quantum Information. Perevod s anglijskogo pod redakciej M.N. Vjalogo i P.M. Ostrovskogo s predisloviem K.A. Valieva // Moskva «MIR». – 2006. C. 311–320.