
Атака на восстановление квантового ключа
ШАХУПОВ Н.Р

Никита Шахулов

Атака на восстановление квантового ключа

«Издательские решения»

Шахулов Н.

Атака на восстановление квантового ключа / Н. Шахулов — «Издательские решения»,

ISBN 978-5-00-554887-0

Все больше внимания уделяется квантовой безопасности легких блочных шифров. Однако, существующие квантовые атаки на облегченные блочные шифры сосредоточены только на квантовом исчерпывающем поиске, в то время как квантовые атаки, в сочетании с классическими методами криптоанализа, не были хорошо изучены. В этой статье мы изучаем атаку на восстановление квантового ключа с использованием алгоритма квантового усиления амплитуды в модели Q1.

ISBN 978-5-00-554887-0

© Шахулов Н.
© Издательские решения

Содержание

Исследования Атак квантового восстановления ключа 6
Абстрактный 6
Вступление 7
Конец ознакомительного фрагмента. 10

Атака на восстановление квантового ключа

Никита Шахулов

© Никита Шахулов, 2021

ISBN 978-5-0055-4887-0
Создано в интеллектуальной издательской системе Ridero

Исследования Атак квантового восстановления ключа

Абстрактный

Квантовая безопасность легких блочных шифров привлекает все больше внимания. Однако существующие квантовые атаки на легкие блочные шифры сосредоточены только на квантовом исчерпывающем поиске, в то время как квантовые атаки в сочетании с классическими методами криптоанализа изучены недостаточно. В этой статье мы изучим атаку квантового восстановления ключа на SIMON32 / 64 с использованием алгоритма квантового амплитудного усиления в модели Q1. Сначала я повторно проанализирую сложность квантовой схемы квантового исчерпывающего поиска на SIMON32 / 64. Я более точно оценю количество ворот Клиффорда и уменьшаем количество T-ворот. Кроме того, T-образная и полная глубина уменьшены из-за наших незначительных изменений. Затем, используя в качестве отличителя четыре дифференциала, данные Бирюковым в FSE 2014, я проверю атаку восстановления квантового ключа на 19-раундовой SIMON32 / 64. Я рассматриваю две фазы атаки восстановления ключа как два экземпляра QAA по отдельности, а первый экземпляр QAA состоит из четырех экземпляров sub-QAA. Затем я проектирую квантовую схему этих двух экземпляров QAA и оцениваю соответствующую им сложность квантовой схемы. Я пришёл к выводу, что квантовая схема моей атаки с квантовым восстановлением ключа ниже, чем квантовый исчерпывающий поиск. Моя работа в первую очередь изучает квантовую специализированную атаку на SIMON32 / 64. И это первая работа по изучению сложности квантовых специализированных атак с точки зрения сложности квантовых схем, которая представляет собой более детальный анализ сложности квантовых специализированных атак. Я проектирую квантовую схему этих двух экземпляров QAA и оцениваю соответствующую им сложность квантовой схемы. Я пришёл к выводу, что квантовая схема моей атаки с квантовым восстановлением ключа ниже, чем квантовый исчерпывающий поиск. Моя работа в первую очередь изучает квантовую специализированную атаку на SIMON32 / 64. И это первая работа по изучению сложности квантовых специализированных атак с точки зрения сложности квантовых схем, которая представляет собой более детальный анализ сложности квантовых специализированных атак. мы проектируем квантовую схему этих двух экземпляров QAA и оцениваем соответствующую им сложность квантовой схемы. Я пришёл к выводу, что квантовая схема моей атаки с квантовым восстановлением ключа ниже, чем квантовый исчерпывающий поиск. Моя работа в первую очередь изучает квантовую специализированную атаку на SIMON32 / 64. И это первая работа по изучению сложности квантовых специализированных атак с точки зрения сложности квантовых схем, которая представляет собой более детальный анализ сложности квантовых специализированных атак.

Ключевые слова: Квантовый криптоанализ, Легкие блочные шифры, Квантовое усиление амплитуды, Дифференциальный криптоанализ, Атака восстановления ключа, SIMON32 / 64

Вступление

Развитие квантовых вычислений представляет угрозу для классических криптосистем. Алгоритм Шора (Shor1994 г.) может нарушить безопасность криптосистем с открытым ключом, основанных на целочисленной факторизации и дискретном логарифме, что приводит к постквантовой криптографии. Что касается симметричных криптосистем, до алгоритма Саймона (Simon1997 г.) применяется в квантовом криптоанализе, есть только алгоритм Гровера (Grover 1997 г.), что помогает получить квадратичное ускорение.

Квантовому криптоанализу блочных шифров в последние годы уделяется много внимания. Следуя представлениям о

Безопасность PRF в квантовых условиях, предложенная Zhandry et al. (Жандры2012 г.), в квантовом криптоанализе существуют две модели защиты от блочных шифров, которые Каплан и др. назвали моделью Q1 и моделью Q2. в (Kaplan et al.2016b).

Модель Q1: Злоумышленнику разрешено только выполнять классические онлайн-запросы и выполнять квантовые автономные вычисления.

Модель Q2: Злоумышленник может выполнять квантовые вычисления в автономном режиме и делать запросы квантовой суперпозиции в режиме онлайн. То есть злоумышленник может запросить оракулу в состоянии суперпозиции и получить состояние суперпозиции в качестве результата запроса.

Мы можем заметить, что модель Q1 более реалистична, чем модель Q2, по той причине, что оракул должен разрешить доступ к суперпозиции. Тем не менее, по-прежнему имеет смысл изучить модель Q2, чтобы подготовиться к будущему с высокоразвитой технологией квантовой связи.

Фактически, квантовый криптоанализ в модели Q2 существует уже давно. В 2010 году Кувакадо и Мори построили квантовый различитель на 3-круговой структуре Фейстеля (Kuwakado and Morii2010 г.) с использованием алгоритма Саймона в модели Q2. Затем они также восстановили ключ Even-Mansour, также используя алгоритм Саймона в 2012 году (Kuwakado and Morii2012 г.). На Crypto2016 Каплан и др. расширили результат в (Kuwakado and Morii2010 г.; 2012 г.) и применил алгоритм Саймона для атаки на ряд режимов шифрования и аутентифицированного шифрования, таких как CBC-MAC, PMAC, OCB (Kaplan et al. 2016a). В модели Q2 алгоритм Саймона может быть объединен с алгоритмом Гровера для применения в квантовом криптоанализе против блочных шифров. Леандер и Мэй (2017 г.) впервые использовал эту идею для атаки на FX-конструкцию в модели Q2. Вдохновленные этой работой, Донг и др. (2020a) дала атаку квантового восстановления ключа на полный цикл ГОСТ также в модели Q2. Кроме того, алгоритм Бернштейна-Вазарани (BV) (Bernstein and Vazirani1997 г.) также может быть применен в квантовом криптоанализе. Ли и Ян (2015 г.) предложил два метода выполнения квантового дифференциального криптоанализа на основе алгоритма BV. Затем Се и Ян расширили результат на Ли и Ян (2015 г.) и представить несколько новых методов атаки на блочные шифры с использованием алгоритма BV (Xie and Yang 2019 г.).

В модели Q1 кажется, что квантовый криптоанализ становится менее мощным. Самая тривиальная квантовая атака – это квантовый исчерпывающий поиск, который определяет общую безопасность блочных шифров в квантовой среде. Грассл и др. представляют квантовые схемы для реализации исчерпывающего поиска ключей на AES и оценки квантовых ресурсов в модели Q1 (Grassl et al.2016 г.). После этого есть также некоторые другие результаты, исследующие квантовую схему AES (Almazrooie et al.2018 г.; Jaques et al.2020 г.; Zou et al.2020 г.;

Langenberg et al.2020 г.). Кроме того, существует множество попыток квантовых специализированных атак в сочетании с классическими методами криптоанализа, например дифференциальным и линейным криптоанализом (Kaplan et al.2016b), атаки встречей посередине (Хосоямада и Сасаки 2018 г.; Bonnetain et al.2019 г.) и рикошетные атаки (Хосоямада и Сасаки 2020 г.; Донг и др.2020b).

За последнее десятилетие исследованиям легковесных блочных шифров было уделено много внимания. Исследователи предложили несколько легких примитивов, чтобы назвать некоторые из них, SIMON (Beaulieu et al.2015 г.), SPECK (Beaulieu et al. 2015 г.), СКИННИ (Beierle et al. 2016 г.), НАСТОЯЩЕЕ (Богданов и др. 2007 г.). Чтобы подготовиться к будущему с крупномасштабными квантовыми компьютерами, необходимо изучить квантовую безопасность легких блочных шифров. Было предпринято несколько попыток изучить общие квантовые атаки на некоторые легкие блочные шифры (Anand et al.2020c; Jang et al.2020 г.; Ананд и др.2020b). В этой статье мы сосредоточимся на квантовой безопасности SIMON. Семейство алгоритмов SIMON (Beaulieu et al.2015 г.) – это легкий блочный шифр, предложенный NSA в 2013 году и обладающий выдающейся производительностью аппаратной реализации. В классической обстановке было много специализированных атак, направленных на SIMON. Однако в квантовой ситуации единственная квантовая атака на SIMON описана в Anand et al. (2020c), где Ананд и др. представить квантовую схему алгоритма Гровера на вариантах SIMON и дать соответствующую оценку квантовых ресурсов, которая является общей квантовой атакой. Для дальнейшего изучения квантовой безопасности SIMON нам необходимо изучить специальные квантовые атаки SIMON. Примечательно, что при измерении сложности атаки все существующие квантовые специализированные атаки изучали сложность шифрования, в то время как в нашем исследовании мы впервые использовали стоимость ресурсов квантовой схемы в качестве меры сложности.

Модель атаки Мы рассматриваем атаку выбранного открытого текста на SIMON32 / 64 в модели Q1, где злоумышленник может делать классические онлайн-запросы оракула шифрования и может выбирать пары случайных сообщений с входным дифференциалом x. Чтобы осуществить такую атаку, противнику необходимо осуществить трансформацию:

qq

$$\sum |0\rangle|0\rangle|0\rangle \rightarrow \sum |m_i\rangle|0\rangle|0$$

*я*знак равно1 *я*= 1

q

→ | mi |*E* |

$$(m_i) \quad E(m_i \oplus \Delta x)$$

я= 1

когда задано q пар классической пары открытый текст-зашифрованный текст в качестве входных данных. Мы полагаем, что этот процесс эффективен. Таким образом, мы можем игнорировать стоимость квантовых ресурсов этого процесса.

Мой вклад В этой статье я изучаю атаку квантового восстановления ключа на SIMON32 / 64 с использованием квантового амплитудного усиления (QAA) в модели Q1. Наш вклад можно резюмировать в следующих двух аспектах.

– Я повторно анализирую сложность квантовой схемы квантового поиска мастер-ключа на SIMON32 / 64. С одной стороны, я далаю более точный результат оценки количества ворот Клиффорда и уменьшенного количества ворот T. Я уменьшаю количество операций процесса расширения ключа, что снижает количество вентилей NOT и CNOT. Кроме того, подсчет ворот Клиффорда, разложенных по воротам Тоффоли, на общее количество ворот Клиффорда, помог мне дать более точную оценку количества ворот Клиффорда. И я уменьшаю количество T-вентилей, используя декомпозицию мультиуправляемых вентилей HE на вспомогательные кубиты. С другой стороны, я даю более тщательный анализ глубины схем. Глубина, на которой я здесь обращаю внимание, – это глубина таких квантовых схем, которые состоят только из вентилей Клиффорда + T. Вносим некоторые модификации в код реализации SIMON32 / 64, что уменьшает Tdepth и полную глубину контуров. По сравнению с (Анандом

и другие. 2020c), я даю более точный и тщательный анализ сложности квантовой схемы QMKS.

– Я представляю мою атаку с квантовым циклическим восстановлением ключа на SIMON32 / 64 с 19 этапами в сочетании с CRKR в

(Бирюков и др. 2014 г.). Я рассматриваю фазу частичного угадывания ключа и фазу исчерпывающего поиска как два экземпляра QAA по отдельности и проектируем соответствующую квантовую схему. Первый экземпляр QAA включает в себя четыре экземпляра суб-QAA, соответствующих четырем процессам восстановления ключа с использованием четырех дифференциалов. Затем оценим

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, купив полную легальную версию на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.