Денисов Н.А. Подготовка криптографических систем к пост-квантовому миру // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 8(46) с. 64–69

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ПОДГОТОВКА КРИПТОГРАФИЧЕСКИХ СИСТЕМ К ПОСТ-КВАНТОВОМУ МИРУ

Денисов Н.А.
ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», г. Москва, Россия (119454, г. Москва, Пр-т Вернадского, д. 78, стр.4), e-mail: ndenisoff@icloud.com

В последние годы было проведено значительное количество исследований в области квантовых компьютеров. Машины, которые используют квантово-механические явления для решения математических задач трудных или неразрешим для обычных компьютеров. Если когда-нибудь появятся крупномасштабные квантовые компьютеры, они смогут взломать многие из используемых в настоящее время криптосистем с открытым ключом. Этот серьезно поставит под угрозу конфиденциальность и целостность цифровых коммуникаций на Интернет. Цель постквантовой криптографии (также называемой квантово-устойчивой криптографией) заключается в разработке криптографических систем, защищенных как от квантовых, так и от классических компьютеров, которые могут взаимодействовать с существующими протоколами связи и сетями.

Ключевые слова: Пост квантовая криптография; криптография с открытым ключом; квантовые вычисления; квантовая устойчивость; квантовая безопасность.

PREPARING CRYPTOGRAPHIC SYSTEMS FOR THE POST-QUANTUM WORLD

Denisov N.A.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ndenisoff@icloud.com

In recent years, a significant amount of research has been conducted in the field of quantum computers. Machines that use quantum mechanical phenomena to solve mathematical problems difficult or unsolvable for ordinary computers. If large-scale quantum computers ever appear, they will be able to crack many of the currently used public key cryptosystems. This will seriously compromise the privacy and integrity of digital communications on the Internet. The goal of post-quantum cryptography (also called quantum-stable cryptography) is to develop cryptographic systems that are protected from both quantum and classical computers that can interact with existing communication protocols and networks.

Keywords: Post-quantum cryptography; public key cryptography; quantum computing; quantum stability; quantum security.

Введение

Постквантовая криптография, также известная как квантовое шифрование, представляет собой разработку криптографических систем для классических компьютеров, которые могут предотвращать атаки, запускаемые квантовыми компьютерами [1].

В 1980-х годах учёные предположили, что, если компьютеры смогут воспользоваться уникальными свойствами квантовой механики, они смогут выполнять сложные вычисления быстрее, чем классические бинарные компьютеры. Быстро стало ясно, что квантовый компьютер, используя преимущества квантовых свойств, таких как суперпозиция и запутанность, может выполнять определенные типы сложных вычислений за считанные часы — то, на что классическому компьютеру потребовалось бы несколько лет.

В 1990-х годах, после того как математик Питер Шор успешно продемонстрировал, что теоретический квантовый компьютер может легко взломать алгоритм, используемый для шифрования с открытым ключом (PKE), криптографы всего мира начали исследовать, как будет выглядеть система постквантовой криптографии.

Доквантовая, квантовая и постквантовая криптография

Квантовые компьютеры используют законы квантовой механики для обработки информации в квантовых битах (кубитах). Поскольку каждый кубит может представлять собой комбинацию нулей и единиц, квантовый компьютер может обрабатывать переменные экспоненциально быстрее, чем классический компьютер.

Доквантовая криптография использует особый тип шифрования, называемый алгоритмом, для преобразования человекочитаемых данных в секретный код. Задача доквантовой криптографии состоит в том, чтобы сделать шифры простыми для понимания, но трудными для обратного проектирования.

Квантовая криптография опирается на физические свойства атомов и использует геометрические шифры для преобразования удобочитаемых данных в секретный код. Основная проблема постквантовой криптографии заключается в том, что квантовая физика является новой научной областью исследований, а создание и эксплуатация прототипов квантовых компьютеров дороги.

Пост квантовая криптография

За последние три десятилетия криптография с открытым ключом стала незаменимым компонентом нашей глобальной цифровой коммуникационной инфраструктура. Эти сети поддерживают множество приложения, которые важны для нашей экономики, нашей безопасности и нашего образа жизни, такие как мобильные телефоны, интернет - торговля, социальные сети и облачные вычисления. В таком взаимосвязанном мире способность отдельных лиц, предприятий и правительств безопасно общаться имеет первостепенное значение.

Многие из наших наиболее важных протоколов связи основаны главным образом на трех основных криптографических алгоритмах: шифрование с открытым ключом, цифровые подписи и обмен ключами.

В настоящее время эти функциональные возможности в основном реализуются с использованием обмена ключами Диффи-Хеллмана, криптосистемы RSA (Ривест-Шамир-Адлеман) и криптосистем с эллиптической кривой. Их безопасность зависит от сложности некоторых задач теории чисел, таких как факторизация целых чисел или проблема дискретного журнала по различным группам.

В 1994 году Питер Шор из Bell Laboratories показал, что квантовые компьютеры — новая технология, которая использует физические свойства материи и энергии для выполнения вычислений. Она может эффективно решить каждую из этих проблем, тем самым визуализируя все криптосистемы с открытым ключом, основанные на такие предположения бессильны [2]. Таким образом, достаточно мощный квантовый компьютер придаст множество форм современные коммуникации – от обмена ключами до шифрования и цифровой аутентификации – находятся под угрозой.

Открытие того, что квантовые компьютеры можно использовать для решения определенных задач быстрее, чем с использованием классических компьютеров вызвали большой интерес к квантовым вычислениям.

За двадцать лет, прошедших с момента открытия Шора, теория квантовых алгоритмов существенно развилась.

Квантовые алгоритмы, достигающие экспоненциального ускорения, были обнаружены для проблем, связанных с физическим моделированием, теории чисел и топологий. Тем не менее, список задач, допускающих экспоненциальное ускорение за счет квантовых вычислений, остается относительно маленький. Напротив, для более широких классов задач были разработаны более скромные ускорения, связанные с поиском, обнаружением коллизий и оценкой булевых формул. В частности, алгоритм поиска Гровера обеспечивает квадратичное ускорение при решении задач неструктурированного поиска. Пока такое ускорение не делает криптографические технологии устаревшими, оно может привести к требованию ключей большего размера, даже в случае симметричного ключа. (Таблица 1 для краткого обзора.)

Таблица 1. Влияние квантовых вычислений на распространенные криптографические алгоритмы

Криптографический алгоритм	Тип	Цель	Влияние большего ключа на тип клипьютера
AES	Симметрический ключ	Шифрование	Необходим более длинный размер ключа
SHA-2, SHA-3	----------	Хэш-функции	Требуется больший результат
RSA	Открытый ключ	Подписи, ключ учреждение	Больше не безопасно
ECDSA, ECDH (Эллиптическая кривая, Криптография)	Открытый ключ	Подписи, ключ учреждение	Больше не безопасно
DSA (криптография конечных полей)	Открытый ключ	Подписи, ключ учреждение	Больше не безопасно

Обзор квантовостойкой криптографии

Наиболее важными применениями криптографии с открытым ключом сегодня являются цифровые подписи и ключи учреждений. Создание крупномасштабного квантового компьютера сделало бы многие из этих криптосистем с открытым ключом небезопасными. В частности, сюда относятся те, на основе сложности факторизации целых чисел, например, RSA, а также на основе сложности задачи дискретного логарифма. Напротив, влияние на системы с симметричными ключами не будет быть столь же радикальным (Таблица 1). Алгоритм Гровера обеспечивает квадратичное ускорение квантовых вычислений, алгоритмы поиска в сравнении с алгоритмами поиска на классических компьютерах. Мы не уверены, что алгоритм Гровера когда-либо будет практически актуален, но если это так, то удвоение

размера ключа будет достаточно для обеспечения безопасности. Кроме того, было показано, что экспоненциальное ускорение алгоритмов поиска невозможен, что позволяет предположить, что симметричные алгоритмы и хэш-функции должны быть пригодными для использования в квантовую эпоху [3].

Следовательно, поиск алгоритмов, которые считаются устойчивыми к атакам как классических, так и квантовых компьютеров сосредоточились на алгоритмах с открытым ключом. Дадим обзор основных семейств, для которых были предложены постквантовые примитивы. Эти семейства включают те, которые основаны на решетках, кодах и многомерных полиномах, а также ряд других.

Криптография на основе решеток. Криптосистемы, основанные на задачах решетки, получили новый интерес по нескольким причинам. Захватывающие новые приложения (такие как полностью гомоморфное шифрование, обфускация кода и шифрование на основе атрибутов) стали возможными с использованием решетчатой криптографии. Большинство алгоритмов создания ключей на основе решеток относительно просты, эффективны и допускают параллельную обработку. Кроме того, безопасность некоторых решетчатых систем доказуемо надежна.

Криптография на основе кода. В 1978 году была впервые предложена криптосистема МакЭлиса. С тех пор появились и другие системы, основанные на кодах, исправляющих ошибки.

Хотя большинство примитивов на основе кода довольно быстры, они страдают от очень больших размеров ключей. В более новых вариантах коды стали более структурированными в попытке сократить количество ключей.

Однако добавленная структура также привела к успешным атакам на некоторые предложения. Пока были некоторые предложения по подписям на основе кода, криптография на основе кода видела больше успеха со схемами шифрования.

Многомерная полиномиальная криптография. Эти схемы основаны на сложности решения системы многочленов многих переменных над конечными полями. Несколько многомерных криптосистем были предложены за последние несколько десятилетий, многие из них были сломаны [6]. Хотя были некоторые предложения по схемам многомерного шифрования. Многомерная криптография исторически более успешна в качестве подхода к подписям.

Подписи на основе хэша. Подписи на основе хеша — это цифровые подписи, созданные с использованием функции хеша. Их безопасность, даже против квантовых атак, хорошо понятна. Многие из более эффективных схем подписи на основе хэша имеют тот недостаток, что подписывающая сторона должна вести учет точного количества ранее подписанных сообщений, и любая ошибка в этой записи приведет к сбою. Еще одним недостатком является то, что можно создать лишь ограниченное количество подписей. Количество подписей может быть увеличено, даже практически неограниченно, но это также увеличивает размер подписи.

Другие виды шифрования. Было предложено множество систем, не подпадающих под вышеперечисленные семейства. Одно такое предложение основано на оценке изогений на суперсингулярных эллиптических кривых. В то время как задача дискретного логарифма на эллиптических кривых может быть эффективно решена с помощью алгоритма Шора для квантового компьютера, проблема изогении на суперсингулярных кривых не имеет

аналогичной известной квантовой атаки. Кажется, маловероятным, что какой-либо из известных на данный момент алгоритмов может служить в качестве подключаемого модуля в замен тому, что используется сегодня. Одна из проблем, которую, вероятно, придется преодолеть, заключается в том, что большинство квантовоустойчивых алгоритмов имеют больший размер ключей, чем алгоритмы, которые они будут использовать. Это может привести к необходимости изменения различных интернет-протоколов, таких как транспортный протокол.

Прогресс в разработке оборудования для квантовых вычислений

Исследования возможности создания крупномасштабных квантовых компьютеров начались всерьез после открытия Питером Шором в 1994 году квантового алгоритма с полиномиальным временем для факторизации целых чисел [2]. В то время было неясно, станут ли квантовые вычисления когда-нибудь фундаментальным изобретением. Многие ведущие эксперты полагали, что квантовые состояния слишком хрупкие и с учетом накопления ошибок для крупномасштабных квантовых вычислений, которые когда-либо будут реализованы.

Ситуация изменилась в конце 1990-х годов с разработкой квантовых кодов, исправляющих ошибки и пороговые теоремы [1]. Эти пороговые теоремы показывают, что, если частота ошибок на логическую операцию («квантовые ворота») в квантовом компьютере можно опустить ниже фиксированного порога, тогда квантовые вычисления произвольной длины могут выполняться надежным и отказоустойчивым способом путем включения этапов исправления ошибок на протяжении всего выполнения квантовых вычислений [4].

С годами экспериментаторы постепенно разрабатывали улучшенное оборудование со все более низкими коэффициентами ошибок на квантовый вентиль. Одновременно теоретики разработали новую процедуры коррекции квантовой ошибки, обеспечивающую более высокие пороги отказоустойчивости. В последнее время некоторые эксперименты с помощью ионных ловушек и сверхпроводящих схем продемонстрированы универсальные наборы квантовых вентилей, которые номинально ниже самых высоких теоретических порогов отказоустойчивости (около 1 %) [6].

Это важная веха, которая стимулировала увеличение инвестиций со стороны правительства и промышленности. Однако очевидно, что необходимы значительные долгосрочные усилия для перехода от современных лабораторных демонстраций, включающие от нескольких кубитов до крупномасштабных квантовых компьютеров, включающих в себя тысячи логических кубитов, закодированных, возможно, в сотнях тысяч или миллионов физических кубитов.

Параллельно с разработкой цифровых квантовых компьютеров общего назначения были произведены усилия по разработке аналоговых квантовых компьютеров специального назначения, таких как квантовые отжигатели (например, машина D-Wave), аналоговые квантовые симуляторы и устройства для отбора проб бозонов. Однако из-за своей специализированной природы эти аналоговые квантовые устройства не относятся к криптоанализу.

Заключение

Вопрос о том, когда будет построен крупномасштабный квантовый компьютер, является сложным и спорным.

Имеется примерно 20 лет на развертывание нашей современной инфраструктуры шифрования с открытым ключом. Это потребует значительного усилия по обеспечению плавного и безопасного перехода от ныне широко используемых криптосистем к их устойчивым к квантовым вычислениям аналогам. Поэтому независимо от того, сможем ли мы оценить точное время наступления эры квантовых вычислений, мы должны начать уже сейчас готовить наши системы информационной безопасности к противостоянию квантовым вычислениям.

Список литературы

1. J. Preskill, Reliable Quantum Computers, Proc. Roy. Soc. London A, 454, 1998, pp. 385–410. http://dx.doi.org/10.1098/rspa.1998.0167
2. P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., 26 (5), 1997, pp. 1484–1509. http://dx.doi.org/10.1137/s0036144598347011.
3. M. Mosca, Cybersecurity in an era with quantum computers: will we be ready? IACR Cryptology ePrint Archive Report 2015/1075, 2015. http://eprint.iacr.org/2015/1075.
4. Голкина Г.Е., Шайтура С.В. Безопасность бухгалтерских информационных систем – Учебное пособие - Бургас, 2016
5. Шайтура С.В., Минитаева А.М., Феоктистова В.М., Ордов К.В. Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М: МГТУ им. Н.Э. Баумана, 2019, с. 377 - 379
6. R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, Y. Chen, B. Chiaro, J. Mutus, C. Neil, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature 508 (7497), 2014, pp. 500–503. http://dx.doi.org/10.1038/nature13171.

References

1. J. Preskill, Reliable Quantum Computers, Proc. Roy. Soc. London A, 454, 1998, pp. 385–410. http://dx.doi.org/10.1098/rspa.1998.0167
2. P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., 26 (5), 1997, pp. 1484–1509. http://dx.doi.org/10.1137/s0036144598347011.
3. M. Mosca, Cybersecurity in an era with quantum computers: will we be ready? IACR Cryptology ePrint Archive Report 2015/1075, 2015. http://eprint.iacr.org/2015/1075.
4. Golkina G.E., Shaitura S.V. Security of accounting information systems – Textbook - Burgas, 2016
5. Shaitura S.V., Minitaeva A.M., Feoktistova V.M., Ordov K.V. Secure information technologies. Proceedings of the Tenth International Scientific and Technical Conference - Moscow: Bauman Moscow State Technical University, 2019, pp. 377-379
6. R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, Y. Chen, B. Chiaro, J. Mutus, C. Neil, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature 508 (7497), 2014, pp. 500-503. http://dx.doi.org/10.1038/nature13171 .