Когда наконец появятся практические квантовые вычисления, они смогут взломать стандартные цифровые коды, защищающие конфиденциальность и безопасность в интернете для правительств, корпораций и практически всех, кто пользуется интернетом.Вот почему правительственное агентство США бросило вызов исследователям, чтобы разработать новое поколение квантово-устойчивых криптографических алгоритмов.

Многие эксперты не ожидают, что квантовый компьютер, способный выполнять сложные вычисления, необходимые для взлома современных стандартов криптографии, станет реальностью в течение ближайших 10 лет. Но Национальный институт стандартов и технологий США (NIST) хочет остаться впереди, получив новые криптографические стандарты, готовые к 2022 году. Агентство осуществляет надзор за вторым этапом процесса стандартизации постквантовой криптографии, чтобы сузить круг лучших кандидатов для квантово-устойчивых алгоритмов, которые могут заменить современную криптографию.

” В настоящее время неразрешимые вычислительные проблемы, которые защищают широко развернутые криптосистемы, такие как RSA и схемы на основе эллиптических кривых, как ожидается, станут разрешимыми",-говорит Рафаэль мисочки, криптограф корпорации Intel и член двух команд (названных Bike и Classic McEliece), участвующих в процессе NIST. "Это означает, что квантовые компьютеры имеют потенциал, чтобы в конечном итоге нарушить большинство безопасных коммуникаций на планете.”

Misoczki был одним из более чем 250 зарегистрированных участников, которые подписались на вторую конференцию по стандартизации PQC, проходившую в Калифорнийском университете в Санта-Барбаре с 22 по 25 августа. На мероприятии были представлены презентации почти всех команд, работающих над 26 алгоритмами кандидатов, которые были отобраны из 69 кандидатов первого раунда.

NIST надеется, что эти кандидаты второго раунда выйдут за рамки простых доказательств концепции и начнут бенчмаркинговые тесты. Ставки высоки, учитывая, что прорыв в области квантовых вычислений может угрожать подорвать безопасность сотен миллиардов долларов только в электронной торговле-не говоря уже о триллионах долларов, находящихся под угрозой в более широкой цифровой экономике. Тем не менее, многие исследователи предупреждают, что NIST должен не торопиться, чтобы оценить новый класс кандидатов для постквантовой криптографии, прежде чем выбирать каких-либо финалистов.

Познакомьтесь с квантово-устойчивыми алгоритмами

Процесс NIST рассматривает алгоритмы, которые попадают в две общие категории, объясняет мисочки. Первая категория включает алгоритмы установления ключа, которые позволяют двум сторонам, которые никогда не встречались, договориться об общем секрете. Эта категория также включает алгоритмы шифрования с открытым ключом—такие как RSA и криптография с эллиптической кривой, которые делают то же самое, но менее эффективны.

Вторая категория включает алгоритмы для цифровых подписей, которые обеспечивают подлинность данных. Такие цифровые подписи используются в приложениях для подписания кода, которые устанавливают уверенность в том, что программа была создана предполагаемым разработчиком, а не хакером.

Обе категории требуют новых алгоритмов, основанных на математических задачах, которые даже квантовые компьютеры не смогли бы взломать. Существует несколько подходов к алгоритмам постквантовой криптографии, каждый из которых имеет свои плюсы и минусы. Например,” такие семейства, как криптография на основе кода, имеют долгую историю общественного контроля, в то время как криптография на основе решетки предлагает очень быстрые алгоритмы",-говорит мисочки.

Компромиссы между каждым подходом могут иметь значительные реальные последствия для вычислительных приложений и устройств. Решетчатая криптография даже быстрее, чем современные криптографические подходы, такие как RSA, но ее больший размер данных может иметь значение, если пропускная способность относительно ограничена.

Вот почему для NIST имеет смысл стандартизировать алгоритмы из нескольких различных подходов, говорит Вадим Любашевский, исследователь криптографии в исследовательской лаборатории IBM Zurich в Швейцарии и участник процесса NIST. “Даже если бы мы были уверены, что все они в безопасности, ни один кандидат не является лучшим в каждой области”, - говорит Любашевский.

Многое остается неизвестным об этих алгоритмах-кандидатах, которые, вероятно, заменят большую часть мировой инфраструктуры, лежащей в основе безопасной глобальной связи, говорит Питер Швабе, исследователь компьютерной безопасности в Университете Радбуда в Нидерландах. Необходима дополнительная разработка и тестирование, чтобы оценить фактическую криптографическую безопасность каждого алгоритма против наилучших возможных атак, измерить компромиссы между безопасностью и производительностью, разработать методы для безопасной реализации алгоритмов и найти вещи, которые могут пойти не так при их развертывании.

” То, что кажется совершенно ясным к настоящему времени, заключается в том, что новые схемы имеют значительно отличающиеся характеристики производительности, чем те, которые мы используем сегодня, и многие из них имеют тонко отличающиеся свойства безопасности", - говорит Швабе.

Дух сотрудничества и соперничество

Задача NIST объединила как академических исследователей, ориентированных на теоретическую работу, так и экспертов в области технологий, знакомых с реальными потребностями производительности и требованиями безопасности. Агентство первоначально описало его как "процесс, подобный конкуренции", но, похоже, стремится поощрять дух сотрудничества между участниками.

Некоторые исследователи присоединились к нескольким командам, работающим над различными алгоритмами. Например, Любашевский является членом групп, работающих над такими алгоритмами, как CRYSTAL-KYBER, CRYSTALS-DILITHIUM и Falcon. "Швабе" принадлежит семь команд, ориентированных на конкретные алгоритмы: кристаллы-кибер, кристаллы ДИЛИТИУМА, классический McEliece, мясо, SPHINCS+, компании NTRU, и MQDSS.

Команды открыто обмениваются фреймворками и отзывами в одном списке рассылки-подход, который имеет свои преимущества и недостатки. "Некоторые вокальные и иногда откровенно невежливые личности доминируют в списке рассылки, заставляя других колебаться, чтобы внести свою работу или вопросы”, - написал один анонимный участник в ответ на опрос NIST.

Большая часть сообщества, похоже, посвящена совместной работе, говорит мисочки, который наблюдал “скорее кооперативную среду, чем конкурентную ситуацию”, несмотря на некоторые различия во мнениях.

Швабе также описал дух сотрудничества сообщества, но отметил, что некоторые люди, похоже, имеют больше конкурентной полосы. ” К сожалению, некоторые участники не настолько сотрудничают и сосредоточены на продвижении "своих" (часто запатентованных) схем, а не работают как сообщество над поиском лучших схем для стандартизации и использования в будущем", - написал Швабе в электронном письме.

Некоторые из конкурирующих алгоритмов представляют собой относительно незначительные вариации на одних и тех же криптографических подходах. Любашевский предложил NIST сосредоточить внимание участников на общей цели стандартизации, запросив конкретные криптографические функции, которые агентство хочет использовать в алгоритмах-кандидатах.

"Хорошо было бы сказать ‘" смотрите, забудьте имена людей, привязанных к этим вещам, вот те черты, которые мы хотим видеть”, - говорит Любашевский.

Новые Стандарты Постквантовой Криптографии

NIST планирует разработать стандарты для постквантовой криптографии около 2022 года. Но исследователи призвали агентство не торопить процесс проверки всех алгоритмов кандидатов. Их анонимная обратная связь была получена из опроса NIST, который был распространен в конце Второй конференции по стандартизации PQC в августе.

“NIST не должна стремиться завершить процесс и иметь стандарты, написанные к 2022 году", - написал один респондент опроса. “Это просто слишком быстро, чтобы получить правильные ответы.... Требуется гораздо больше исследований.”

Другой респондент опроса предложил, чтобы” NIST отложил создание любого стандарта до 2025 года и финансировал исследовательские усилия, чтобы посмотреть на всех кандидатов до этого времени“, чтобы " дать исследователям шанс на инновации.”

Один из респондентов, участвовавших в опросе, нарисовал особенно мрачную картину возможных последствий стремительного продвижения вперед: “попытка завершить этот процесс всего за пару лет опасна и может привести к катастрофическим результатам и/или потере воспринимаемой легитимности процесса и результатов.”

Многие указывали на необходимость более глубокого криптоанализа для тщательного изучения возможных слабых мест каждого алгоритма. Один человек призвал NIST спонсировать больше академических исследований в университетах США для дальнейшего развития " науки квантового криптоанализа.”

"Проблема криптографии в целом заключается в том, что криптоанализ-это такой неблагодарный процесс”, - говорит Любашевский. - если вы потерпите неудачу, и никто не узнает, что вы пытались и потерпели неудачу, или вы добьетесь успеха и получите свои пять минут славы, а затем этот алгоритм, который вы написали, больше никогда не будет использоваться.”

NIST может частично рассчитывать на идею о том, что разные команды будут пытаться сломать алгоритмы друг друга. Но Любашевский предложил, чтобы агентство также изучило требование к исследователям проверить работу другой группы или, возможно, сделать криптоанализ частью условий финансирования теоретической работы по разработке алгоритмов.

Когда Компьютеры Взломают Криптографию?

Никто точно не знает, когда квантовые вычисления сделают современные криптографические алгоритмы бесполезными. Одна из сложностей заключается в том, что первое правительство или организация, разработавшие практический квантовый компьютер, могли бы многое выиграть, просто храня молчание, взламывая современные криптографические системы и разглашая мировые секреты.

” Я вижу хороший шанс, что первые большие универсальные квантовые компьютеры будут доступны только государственным учреждениям, которые не будут точно рекламировать, что у них есть такие вычислительные возможности", - говорит Швабе. Он видит " реальный шанс, что в течение 20 лет появятся квантовые компьютеры, которые сломают криптографию, которую мы широко используем сегодня.”

Исследователи криптографии знают, что правительствам и промышленным предприятиям мира может потребоваться много времени, чтобы принять новейшие криптографические стандарты. Несмотря на то, что криптография с эллиптической кривой была впервые предложена в конце 1980-х годов, большая часть мира по-прежнему полагается на более старую криптографию RSA, которая появилась в конце 1970-х годов, поэтому по-прежнему существует некоторая актуальность усилий NIST по стандартизации для постквантовой криптографии, даже если практические квантовые вычисления остаются на расстоянии нескольких десятилетий.