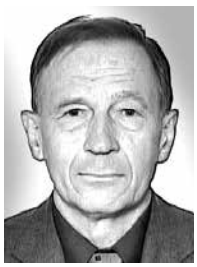
МАТЕМАТИЧЕСКИЕ АСПЕКТЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ



Геннадий Матвеев,
доцент факультета прикладной математики и информатики БГУ, кандидат физико-математических наук

Криптография, представляющая собой практику безопасного общения, предполагает использование математических алгоритмов для преобразования обычного текста в нечитаемый, зашифрованный формат. После чего он пересылается через сеть Интернет, и расшифровывается получателем в обычный текст с помощью ключа.

Преимущества криптосистем с открытым ключом

Понять, что такое криптография, позволяет следующий пример. Алиса и Боб – имена условных персонажей, которые хотят обмениваться сообщениями так, чтобы их содержание оставалось в секрете. Очевидно, что у каждой из сторон должен быть свой ключ. На практике используются два вида криптосистем. К первому относятся симметричные криптосистемы. При этом для шифрования и расшифровывания применяется один и тот же криптографический ключ, который должен храниться в секрете обеими сторонами. Алгоритм шифрования выбирается ими до начала обмена сообщениями. Однако если этот ключ будет скомпрометирован, всякая попытка защитить секретную информацию с его помощью потеряет смысл.

Криптосистема с открытым ключом – это асимметричная схема, в которой применяется пара ключей: открытый (public key), с помощью которого зашифровывают данные, и соответствующий ему закрытый (private key), который применяют при расшифровке. Алиса размещает свой открытый ключ в открытом доступе, в то время как закрытый держит в тайне. Любой человек с копией ее открытого ключа может зашифровать информацию, которую только она и сможет прочитать. Это могут сделать даже люди, с которыми она прежде никогда не встречалась. Для более детального знакомства с этими и другими криптографическими понятиями можно рекомендовать книгу [2].

Исследования по основным направлениям современной криптографии ведутся с 2000 г. в НИИ прикладных проблем математики и информатики БГУ под руководством академика НАН Беларуси Юрия Харина.

Хотя ключевая пара математически взаимосвязана с помощью некоторого уравнения, вычислить закрытый ключ, владея данными об открытом, должно быть практически невыполнимо. Современная математика умеет решать такие задачи. Каждый, у кого есть ваш

открытый ключ, сможет зашифровать данные, но только пользователь, обладающий соответствующим закрытым ключом, может прочитать сообщение.

Главное преимущество асимметричного шифрования в том, что оно позволяет лицам, не имеющим предварительной договоренности о безопасности, обмениваться конфиденциальной информацией. Таким образом, Алисе и Бобу не надо согласовывать секретный ключ по специальному защищенному каналу. Все коммуникации затрагивают только открытые ключи, тогда как закрытые хранятся в безопасности. Примерами криптосистем с открытым ключом являются RSA (названная в честь изобретателей Рона Ривеста, Ади Шамира и Леонарда Адлемана) и Elgamal (названная в честь автора – Тахира Эль-Гамаля) и др.

Симметричная криптография долгое время была единственным способом пересылки секретной информации, а цена надежных каналов для обмена ключами ограничивала ее применение узким кругом организаций, которые могли себе это позволить. Появление шифрования с открытым ключом стало технологической революцией, предоставившей надежную криптографию широкому кругу пользователей. Для полноты картины перечислим и некоторые недостатки асимметричных алгоритмов.

Они используют более длинные ключи, чем симметричные. Разница при этом довольно существенная. Например, 128-битный симметричный ключ и 2048-битный асимметричный обеспечивают примерно одинаковый уровень безопасности. Асимметричное шифрование сравнительно медленнее, чем симметричный алгоритм, а также требует больше вычислительных ресурсов. Поэтому оно неэффективно при передаче длинных сообщений. Эта проблема на практике решается с помощью так называемого механизма инкапсуляции ключей (KEM).

Его при необходимости должны поддерживать современные стандарты асимметричного шифрования. В связи с этим дадим необходимые пояснения.

Протокол KEM относится к классу криптографических алгоритмов, спроектированных для безопасной передачи ключей симметричных криптосистем с помощью криптосистем с открытым ключом. Это вызвано тем, что последние, как уже отмечалось, неудобны для передачи длинных сообщений, и вместо этого используются для обмена симметричными ключами, которыми в итоге шифруется текст. Для этого первоначально был предложен следующий алгоритм:

- *генерируется случайное число w (ключ);*
- *оно шифруется открытым ключом и отправляется получателю;*
- *тот расшифровывает его закрытым ключом и восстанавливает симметричный ключ w.*

К сожалению, данный алгоритм имеет ряд недостатков. Например, злоумышленник может отправить свое число, зашифрованное открытым ключом, и затем обмениваться сообщениями с получателем. На практике инкапсулированный ключ защищают от манипуляций путем добавления кода аутентификации.

Более надежный метод использует подход посложнее. В частности, получатель зашифрованного случайного числа w формирует материал ключа $y = KDF(w)$ для его последующего шифрования. То же самое делает и отправитель. Key Derivation Function – функция, которая служит для получения секретных ключей из какого-то другого секретного значения для задач защиты информации.

ЭЦП, проблема факторизации, RSA

Широко применяемая технология электронной цифровой подписи (ЭЦП) основана на современных стандартах асимметричного шифрования и опирается на следующие принципы.

• Разработаны надежные методы шифрования сообщения закрытым ключом так, что прочитать его можно только связанным открытым. При этом механизм шифрования/расшифрования является общеизвестным.

• Если электронный документ расшифрован с помощью открытого ключа, то можно быть уверенным, что он был зашифрован уникальным закрытым. Если документ прочитан благодаря открытому ключу Алисы, то это подтверждает ее авторство: зашифровать данный документ могла только Алиса, поскольку она – единственный обладатель закрытого ключа.

• Можно сгенерировать пару (открытый и закрытый ключи) так, чтобы, зная первый, нельзя было вычислить второй за разумный срок. Алгоритм генерации ключей строго определен и является общеизвестным. При этом каждому открытому ключу

соответствует закрытый. Если, например, Алиса публикует свой открытый ключ, то это означает, что соответствующий закрытый есть только у нее.

• На практике шифровать документ целиком весьма затратно, поэтому шифруется только его хеш-значение, то есть небольшой объем данных, жестко привязанный к документу с помощью математических преобразований и идентифицирующий его. Механизм хеширования строго определен и является общеизвестным. Шифрованное хеш-значение и является электронной подписью.

Термины «цифровая подпись», «электронная подпись» и «ЭЦП» – синонимы. Данное понятие было впервые предложено в 1976 г. У. Диффи и М. Хеллманом, хотя это была всего лишь идея. Годом позже был разработан алгоритм RSA, который без дополнительных модификаций можно использовать для создания цифровых подписей. Вскоре после RSA разработали другие ЭЦП, такие как алгоритмы цифровой подписи М. Рабина и Р. Меркла.

Стойкость всякой схемы ЭЦП и асимметричного шифрования основана на вычислительной сложности некоторой математической задачи. Для RSA это факторизация целого числа. Определенно можно сказать, что при наличии ее эффективного алгоритма не составит труда найти секретный ключ RSA.

Неизвестно, есть ли эффективный неквантовый алгоритм факторизации целых чисел. Однако доказательств того, что не существует решения этой задачи за полиномиальное время, также нет. Первая большая распределенная факторизация касалась числа RSA-129, имеющего 129 десятичных знаков (426 бит). В 1977 г. его использовали Р. Ривест, А. Шамир и Л. Адлеман, зашифровав фразу из нескольких слов. Они утверждали, что на расшифровку понадобятся триллионы лет, однако ключ к самому сложному на тот момент шифру был найден за 17 лет. Над дешифрованием работали 600 ученых и добровольцев на 5 континентах при помощи 1600 компьютеров. Это число было разложено на два сомножителя в период с сентября 1993 г. по апрель 1994 г. Фактической целью этого проекта было стимулирование изучения проблемы факторизации больших чисел и надежности RSA-криптосистемы в частности.

Квантовые вычисления

Впервые они были предложены независимо Ю.И. Маниным и Р. Фейнманом в начале 1980-х гг. для моделирования сложных квантово-механических систем [1, 5].

Оказалось, что квантовые вычисления могут дать значительное ускорение для решения ряда сложных математических задач, таких как факторизация чисел и дискретное логарифмирование. В 1994 г. П. Шор разработал алгоритм, способный справиться с этими задачами. Он имеет полиномиальную сложность для разложения числа на простые множители и дискретного логарифмирования на квантовом компьютере [6].

В отличие от обычных устройств, работающих на основе полупроводниковых технологий, мощность квантовых значительно выше. Их возможности превосходят любые инструменты, которые сегодня применяют хакеры. Квантовый компьютер использует вместо классических битов (бинарных переменных, единичек и нулей) кубиты – систему с двумя уровнями. Они, в отличие от битов, могут находиться в состоянии 0, 1 и в суперпозиции 0 и 1. На практике это означает, что при наличии квантового компьютера из приблизительно 3 тыс. кубитов криптографическая система RSA с ключом длиной 2048 битов может быть эффективно взломана за время, лишь ненамного превосходящее то, что требуется для шифрования. Это стало существенной проблемой для криптографии, так как безопасность распространенных стандартизированных систем зависит от сложности решения задач разложения числа на простые множители и дискретного логарифмирования.

Квантовые вычисления могут применяться не только в криптографии. С их помощью эффективно решается ряд алгоритмических задач в алгебре, а также предложен протокол генерации общего ключа на квантовом компьютере. Уточним, что лучший классический алгоритм факторизации числа N требует времени, экспоненциально зависящего от n, где $n = log\ N$, а алгоритм Шора [6] на квантовом компьютере – полиномиально зависящего от n, а именно $O(n^2 log_2 n (log_2 log_2 n))$ операций. Отсюда следует возможность экспоненциального ускорения решения проблемы факторизации: на квантовом компьютере для компрометации схемы RSA вместо тысяч лет потребуется несколько часов, дней,

недель, месяцев. Разумеется, сказанное носит пока условный характер, а станет актуальным лишь с появлением работающих квантовых компьютеров.

Для более детального знакомства с квантовыми вычислениями можно рекомендовать книгу [3].

Задача дискретного логарифмирования, как и задача факторизации большого натурального числа,– одна из основных вычислительно трудных, на которых базируется современная криптография. Это обусловлено предположительно высокой сложностью обращения дискретной показательной функции. Хотя задача вычисления дискретной показательной функции решается достаточно эффективно, даже самые современные алгоритмы вычисления дискретного логарифма имеют очень высокую степень сложности, которая сравнима со сложностью факторизации целого числа. Классическими криптографическими схемами на основе задачи дискретного логарифмирования являются схема выработки общего ключа Диффи-Хеллмана, схемы электронной подписи Эль-Гамаля, DSA, EdDSA и др.

Еще одна возможность эффективного решения задачи вычисления дискретного логарифма связана с квантовыми вычислениями. Теоретически доказано, что с помощью алгоритма Шора он вычисляется за полиномиальное время. Можно утверждать, что в случае, если полиномиальный алгоритм нахождения дискретного логарифма будет реализован, криптосистемы на его основе станут практически непригодными для долговременной защиты данных. Квантовые алгоритмы с начала 1980-х гг. остаются лишь потенциальной возможностью, которую пока невозможно технически реализовать в полной мере.

Перспектива создания квантовых компьютеров стимулировала Национальный институт стандартов и технологий США (NIST) объявить открытый конкурс по разработке постквантовых криптографических алгоритмов. Точнее говоря, NIST заинтересован в новых стандартах асимметричного шифрования (Public-Key Encryption) и цифровой подписи (Digital Signatures). Основное требование для алгоритмов постквантовой криптографии состоит в том, что они должны быть основаны на задачах с математически доказанной вычислительной сложностью (NP-сложных). Такие алгоритмы называют постквантовыми или квантово-устойчивыми.

Первоначально на участие в конкурсе подали заявки 69 команд со всего мира. Уже проведены три этапа, определены перспективные направления и произведен конкурсный отбор участников.

В настоящее время разработка алгоритмов постквантовой криптографии ведется по 4 направлениям, использующим: теорию решеток (Lattice based cryptography), коды, исправляющие ошибки (Code based cryptography), многочлены в конечных полях (Multivariate, quadratic equations cryptography), теорию хэш-функций для больших данных (Hash-based cryptography).

К асимметричным системам шифрования в рамках конкурса NIST предъявляются требования по обеспечению стойкости к следующим угрозам различения шифртекстов относительно атак на основе:

- *подобранного открытого текста (Indistinguishability Against Chosen Plaintext Attack, IND-CPA);*
- *подобранного зашифрованного текста (Indistinguishability Against Chosen Ciphertext Attack, IND-CCA);*
- *неадаптивно подобранного открытого текста (Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CPA1);*
- *адаптивно подобранного открытого текста (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CPA2).*

Криптосистема Мак-Элиса

Как показал третий этап конкурса NIST, криптосистема Мак-Элиса Classic McEliece [7] со встроенным кодом Гоппы является одним из кандидатов для последующей стандартизации. Она относится к семейству квантово-устойчивых криптографических алгоритмов, стойкость которых основывается на предположении о вычислительной сложности задачи декодирования случайного линейного кода. В частности, на этой задаче основан не только алгоритм Classic McEliece, но и альтернативные финалисты – алгоритмы BIKE и HQC. Код Гоппы в 1970 г. разработал советский математик В.Д. Гоппа.

Алгоритм Classic McEliece – криптосистема с открытым ключом на основе теории алгебраического кодирования, созданная в 1978 г. Р. Мак-Элисом. Это первая схема, использующая рандомизацию в процессе шифрования. Алгоритм ранее не получил широкого признания в криптографии, но в то же

время является кандидатом для постквантовой криптографии, так как устойчив к атакам на основе алгоритма Шора.

Криптосистема Мак-Элиса строится на тех же принципах, что и криптосистема Г. Нидеррайтера, разработанная последним в 1986 г. и основанная на сложности декодирования полных линейных кодов [8]. Несмотря на то, что данная криптосистема была взломана В. Сидельниковым и С. Шестаковым, некоторые ее модификации остаются криптостойкими [9]. Одна из них лежит в основе алгоритма BIKE-2 – альтернативной схеме асимметричного шифрования и цифровой подписи.

Рассмотрим вариант криптосистемы Мак-Элиса [7, 10], который вошел в третий этап конкурса. Основная идея состоит в маскировании линейного кода под код, не обладающий видимой алгебраической и комбинаторной структурой. Есть 2 разновидности данной криптосистемы: основанная на кодах Гоппы и на БЧХ-кодах. В нашем случае алгоритм построения выглядит следующим образом.

Закрытый ключ состоит из:

- *матрицы G размером k×n, необходимой для генерации кода Гоппы, исправляющего t ошибок;*
- *матрицы перестановок P размером n×n;*
- *случайной невырожденной матрицы S размером k×k.*

Матрицы P и S необходимы для сокрытия структуры открытого ключа, коим является матрица G_{pub} размером $k×n$, вычисляемая исходя из матриц закрытого ключа: $G_{pub}=SGP$. Легко заметить, что в открытом ключе содержится информация о закрытом, но она скрыта. Поэтому невозможно восстановить по открытому ключу закрытый атакой грубой силы за разумное время.

При шифровании случайным образом выбирается вектор длины r над полем $GF(2)$ с весом Хэмминга не более t. Затем идет вычисление шифртекста: $C=mG_{pub}+r$.

Расшифровка производится в три этапа:

- *вычисляется вектор* $c' = cG_{pub}^{-1}$;
- *при помощи алгоритма быстрого декодирования кода Гоппа находится* m', *для которого* $d_H(m'G_{pub}c) \le t$;
- *находится открытый текст* $m = m' S^{-1}$.

Достоинство данного алгоритма состоит в том, что он работает значительно быстрее RSA. Недостатком является большой размер открытого ключа, вследствие чего данная система была ранее малораспространенной. Имеется ряд работ, посвященных анализу этой криптосистемы, благодаря чему она считается хорошо изученной.

Геометрические свойства решетки позволяют рандомизировать еще одного участника конкурса NIST – алгоритм NTRU при помощи преобразования $e =r⊗h+mmodq$.

То есть на определенном этапе используется случайный вектор ошибок r.

Рандомизация считается преимуществом, поскольку она применяется еще и в системах BIKE и SABER.

Современные квантовые компьютеры пока не обладают мощностью, достаточной для взлома систем на основе асимметричного шифрования.

Анализ зарубежной литературы показывает, что полноценный квантовый компьютер можно ожидать лишь в ближайшие десятилетия, а первые случаи квантовых атак могут быть зафиксированы примерно в 2030 г. Наиболее уязвимыми к подобным угрозам считаются персональные и финансовые данные, а также данные, касающиеся блокчейн-экономики [4].

Большинство зарубежных экспертов оценивают квантовую угрозу как реальную. Поэтому назрела необходимость привести систему криптографической защиты информации республики в соответствие с новыми постквантовыми требованиями. Недавно завершившийся международный конкурс постквантовых криптографических алгоритмов выявил общие схемы построения надежных квантово-устойчивых криптосистем, а значит, непреодолимых препятствий для их разработки не существует. НИ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Манин Ю. И. Вычислимое и невычислимое / Ю.И. Манин. – М., 1980.
2. Харин Ю.С. Криптология: учебник / Ю.С. Харин, С.В. Агиевич, Д.В. Васильев, Г.В. Матвеев. – Минск, 2013, 2023.
3. Квантовая криптография: идеи и практика / под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. – Минск, 2008.
4. И. Голдовский. Постквантовая криптография. Готовимся сегодня? // ПЛАС. 2023. №2 (288).
5. Bernstein D., Lange T. Post-quantum cryptography // https://doi.org/10.1038/nature23461.
6. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th Ann. Symp. on Foundations of Computer Science (FOCS'94) 124–134 (IEEE, 1994).
7. McEliece R.J. A Public-Key Cryptosystem based on Algebraic Coding Theory. Deep Space Network Progress Report. P. 42–44.
8. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory (англ.) / H. Niederreiter // Problems of Control and Information Theory. 1986. Vol. 15. Iss. 2. P. 159.
9. V.M. Sidelnikov, S.O. Shestakov. On insecurity of cryptosystems based on generalized ReedSolomon codes // Discrete Mathematics and Applications. 1992. №2 P. 439–444.
10. E. Persichetti. Code-based Key Encapsulation from McEliece's Cryptosystem // arXiv:1706.06306v1, Jun. 2017.