1. Введение

Как следует из названия, базисная функция является частью некоторого базиса в функциональном пространстве. Если базис определен в линейном пространстве, функция также может называться базисным вектором. Набор базисных функций определяет базис пространства, все остальные элементы которого могут быть выражены как линейная комбинация элементов данного базиса. Например, аналитическую функцию от одного переменного можно разложить в ряд Тейлора – бесконечную сумму, где в качестве базисных функций выбраны степенные. Если в качестве базиса взять синусоидальные функции, мы получим преобразование Фурье.

Базисы применяются в кодировании и обработке сигналов, в сжатии информации. В частности, широкое применение нашли вейвлеты – от сжатия изображений до анализа аудио- и видеосигналов. В последнее время, когда теория квантовых компьютеров постепенно воплощается на практике, а сами квантовые компьютеры существуют не только в теории, но и в виде реальных прототипов, базисы пришли и в криптографию. Алгоритмы с использованием базисов гораздо более устойчивы к атакам с помощью квантовых компьютеров, вследствие чего являются достойной заменой современным алгоритмам асимметричной криптографии.

2. Причины использования базисов в криптографии

История применения базисов в компьютерных задачах берет начало еще на заре становления компьютеров, но применять их в криптографии стали относительно недавно. Существующие алгоритмы шифрования, которые

являются в частности государственными стандартами, полностью открыты и доступны для исследования любому желающему. Криптографический алгоритм ГОСТ 28147-89, используемый в России, введен в качестве государственного стандарта еще в 1990 году, и тот факт, что за четверть века в нем не обнаружены серьезные уязвимости, лучше всего говорит о его криптостойкости. Перехватив зашифрованный текст, злоумышленник может лишь использовать атаку грубой силой, перебирая все возможные варианты, что может занять миллионы лет. Единственной проблемой в таком случае является выбор достаточно стойкого и неочевидного ключа шифрования, но это уже проблема передающей стороны, а не криптоалгоритмов.

Проблемы начались с приходом идеи о квантовых компьютерах. В 1980г. Юрий Манин впервые высказал идею о квантовых исчислениях, а спустя всего год Ричард Фейнман предложил первую модель квантового компьютера. Вскоре после этого Пол Бениофф описал теоретические основы построения такого компьютера.

Квантовый компьютер использует для вычислений не классические алгоритмы, а процессы квантовой природы – квантовый параллелизм и квантовую запутанность. Вместо битов данных в нем используются т.н. кубиты. Система из N битов в современном компьютере может принимать только одно состояние в каждый момент времени, а система из N кубитов, вследствие принципа квантовой суперпозиции, до первого измерения находится во всех состояниях одновременно. Пространство состояний такого квантового регистра из N бит является 2^N – мерным гильбертовым пространством, а операция в квантовом исчислении – поворотом вектора состояния регистра в этом пространстве. Таким образом, система фактически задействует одновременно 2^N состояний.

В приложении к криптоанализу квантовый компьютер сможет осуществлять перебор паролей быстрее компьютера обыкновенного, а главное – алгоритмы ассиметричного шифрования, которые в наши дни используются повсеместно,

перестанут обеспечивать хоть какую-то секретность передаваемой информации. Если злоумышленнику известен шифрованный текст (который всегда возможно перехватить) и открытый ключ, по алгоритму Шора квантовый компьютер сможет достаточно быстро вычислить секретный ключ, и далее без каких либо проблем злоумышленник будет просматривать все сообщения, зашифрованные данным секретным ключом.

Созданием алгоритмов, устойчивым к атакам с помощью квантовых компьютеров, занимается особая отрасль криптографии – постквантовая криптография. Алгоритмы с использованием базисов являются одним из наиболее перспективных ее направлений.

Другая область криптографии, в которой могут найти свое применение базисы – квантовая криптография. Данная отрасль занимается построением алгоритмов, основанных на принципах квантовой физики, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Здесь с использованием базисов возможно создание канала передачи данных, защищенного от прослушивания. Информация передается по такому каналу в виде поляризованных фотонов, состояние которых, как известно, нельзя определить, не исказив саму передаваемую информацию. Легальные пользователи по открытому каналу обсуждают переданную и полученную информацию, проверяя тем самым возможность перехвата сообщения. Если ошибок выявлено не будет, такую информацию можно считать секретной.

3. Криптографические алгоритмы с использованием базисов

Наибольшее развитие в данной тематике причинам получила теория решеток, и причин тому несколько. Во-первых, криптографические примитивы на основе

задач теории решеток обладают очень сильной криптостойкостью, основанной на доказательстве «в наихудшем случае». Появление квантовых компьютеров, которые способны обрушить всю современную асимметричную криптографию, никак не повлияет на криптостойкость подобных примитивов. Во-вторых, они сравнительно эффективно выполняются на компьютерах. И в-третьих, такие примитивы чрезвычайно просты в своей формулировке.

Криптостойкость алгоритмов с использованием решеток, как и современных алгоритмов асимметричной криптографии, основана на включении в задачу вскрытия шифртекста трудной математической задачи. У современных алгоритмов это, как правило, задача вычисления дискретного логарифма и факторизация больших чисел. За три десятка лет исследований так и не было найдено алгоритма вычисления логарифма или разложения целого числа на множители за полиномиальное время, однако с приходом квантовых компьютеров ситуация изменится. Алгоритм Шора, разработанный Питером Шором в 1994г., позволяет разложить на множители число M за время $O(lg^3 M)$, используя $O(\lg M)$ кубитов. В 2001г. группа специалистов IBM разложила число 15 на множители 3 и 5 при помощи квантового компьютера с 7 кубитами. Учитывая постоянно растущую скорость развития науки, нельзя с уверенностью сказать, останется ли асимметричная криптография в ближайшем будущем, с появлением прототипов квантовых компьютеров с сотнями и тысячами кубитов.

В основе алгоритмов с использованием решеток лежат проблемы, основанные на результатах работ венгерского математика Миклоша Айтаи, опубликованных им в 1996г. Айтаи доказал, что можно построить случайную решетку с коротким вектором в ней, причем такую, что любой алгоритм нахождения этого вектора в данной решетке можно конвертировать в эффективный алгоритм нахождения достаточно короткого вектора в любой решетке. Эти результаты положили начало новому направлению в криптографии, которое получило название «Lattice based cryptography» или

«Криптография на основе решеток». Одной из вычислительно сложных задач в теории решеток является проблема нахождения ближайшего вектора. Пусть задана некая решетка и некоторый базис на ней. Пусть также задан некий вектор, не принадлежащий решетке. Требуется в данной решетке и при данном базисе найти вектор, максимально схожий по длине с заданным.

В последнее время базисы находят в криптографии все более широкое применение. В 2009г. вышли в свет статья[13] и диссертационная работа[10] А.Б. Левиной, в которых предлагается алгоритм шифрования информации с применением сплайн-вейвлетов. Год спустя А.И. Савватин и С.А. Новоселов предложили алгоритм передачи речевой информации[9], где определенный базисный набор вейвлет-фильтров, преобразующих исходный сигнал, используется в качестве ключа. В 2011г. Д.С. и С.Ф. Лукомские описали[11] алгоритм шифрования информации с использованием базисов с теоретически бесконечным числом вариантов ключей шифрования.

3.1. Алгоритмы передачи данных с защитой от перехвата

Квантовая криптография – динамично развивающееся направление науки, которое открывает множество новых перспектив в традиционных областях в целом и криптографии в частности. Сейчас в подавляющем большинстве реальных систем шифрования применяются симметричные и ассиметричные алгоритмы. Обоим видам алгоритмов свойственны свои достоинства и недостатки. При симметричном шифровании передающей и принимающей стороне необходимо заранее согласовывать выбранный ключ, что создает угрозу его перехвата на данном этапе. Ассиметричное шифрование лишено этого недостатка, но появление квантовых компьютеров лишит все

современные алгоритмы данного вида, сложность вскрытия которых основана на задаче факторизации или нахождения дискретного логарифма, хоть какой-то криптостойкости. Одной из альтернатив является переход на алгоритмы, предложенные в предыдущем разделе. Другое решение – симметричное шифрование с передачей ключа по алгоритмам квантовой криптографии. Их уникальность заключается в том, что впервые в истории мы можем говорить об абсолютной секретности. В современных алгоритмах при передаче информации никогда нельзя гарантировать, что она не была перехвачена и/или модифицирована в результате атаки «человек посередине». При передаче информации по протоколам квантовой криптографии передающая и принимающая сторона могут судить о том, был перехват информации или нет, по характеру пришедшей принимающей стороне информации и количеству ошибок при передаче.

По формулировке авторов протокола BB84, квантовая криптография – это метод передачи информации, позволяющий двум пользователям по каналу связи согласовать ключ для симметричного шифрования без изначального знания каких-либо секретов, известных только данным пользователям, причем ключ останется секретным для злоумышленников, пытающихся осуществить перехват информации при передаче.

BB84 использует для кодирования четыре состояния двухуровневой квантово-механической системы, формируя два сопряженных базиса. Обозначим эти базисы индексами a и b. Получаем $(|0_a\rangle; |1_a\rangle)$ и $(|0_b\rangle = \frac{1}{\sqrt{2}}(|0_a\rangle + |1_a\rangle); |1_b\rangle = \frac{1}{\sqrt{2}}(|0_a\rangle - |1_a\rangle))$. Состояния $|0_a\rangle$ и $|1_a\rangle$ кодируют значения 0 и 1 в базисе a, а $|0_b\rangle$ и $|1_b\rangle$ – 0 и 1 в базисе b. Геометрически базис b можно представить как поворот базиса a на $\frac{\pi}{4}$. Оба они ортогональны, поэтому если измерения проводятся в пределах одного базиса, два состояния системы можно надежно различить. Однако если передающая и принимающая сторона проводят измерения в разных базисах, результат будет случайным.

Обмен информации осуществляется в две стадии: сперва по квантовому каналу, затем – по обычному, в том числе открытому для перехвата. Единственным условием для данного канала является невозможность модификации передаваемой информации.

Сначала Алиса случайно и с равной вероятностью выбирает одно из четырех состояний системы и пересылает его Бобу по квантовому каналу, запоминая значение бита и базис, в котором он закодирован. Боб тоже выбирает базис (случайно и независимо от Алисы) и запоминает результат своих измерений. Если базисы Алисы и Боба одинаковы, то значения совпадут. В ином случае они совпадут с вероятностью 1/2. Алиса и Боб повторяют процедуру N раз, в результате чего каждый из них будет обладать N битами данных. Затем по открытому каналу они сообщают друг другу, какие базисы использовали для каждого конкретного бита, и выбрасывают из переданного сообщения те биты, для которых базисы не совпали. После этого у них остается примерно N/2 бит. Эти данные называются сырым ключом.

Представим, что Ева перехватывает носители информации, отправленные Алисой, после чего измеряет их состояние и пересылает далее Бобу. Поскольку при несовпадении базисов биты будут исключены из финального ключа, брать в расчет можно только те биты, для которых базисы Алисы и Боба идентичны. Так как Ева будет выбирать базисы независимо от Алисы и Боба, примерно в половине случаев базисы Евы будут не совпадать с базисами Боба. При этом результаты измерений Боба будут примерно в половине случаев не совпадать с результатами Алисы. В итоге измерения Боба будут давать верный результат с вероятностью (1/2 + 1/2 * 1/2), хотя в отсутствие Евы такая вероятность была бы равна единице. Таким образом, чтобы выяснить, имел ли место перехват информации, Алиса и Боб должны сравнить по открытому каналу связи некоторое число бит, для которых их базисы совпали. Если ошибки присутствуют, значит, информация была перехвачена. В таком случае все данные отбрасываются, и процесс передачи информации начинается сначала.

Если ошибок нет, переданную информацию можно считать секретной. Участвовавшие в проверки биты отбрасываются, и оставшиеся формируют секретный ключ.

Выше мы рассматривали модель идеального бесшумного квантового канала, однако на практике даже в отсутствие подслушивания будет иметь место некоторое несоответствие данных Алисы и Боба, которые в теории должны совпадать. Алиса и Боб должны производить оценку процента ошибок при передаче: если она выходит за некий порог, считается, что информация была перехвачена. В противном случае Алиса и Боб переходят к исправлению ошибок.

Предложены методы для упрощения системы передачи данных по квантовому протоколу[1, 2].

Анализ атак на квантовые протоколы приведен в [3, 4, 21].

В 1992г. Беннетом был введен протокол передачи данных B92. Он показал, что в квантовой криптографии могут быть использованы любые два неортогональных состояния. Обозначим их $|\Psi_0\rangle$ и $|\Psi_1\rangle$ – два состояния, соответственно кодирующие 0 и 1. Их произведение $\|\langle\Psi_0|\Psi_1\rangle\|^2$ лежит в интервале от 0 до 1. Алиса отправляет Бобу случайно выбранное состояние, после чего Боб применяет к нему случайно выбранный оператор проектирования $P_0 = 1 - |\Psi_1\rangle\langle\Psi_1|$ или $P_1 = 1 - |\Psi_0\rangle\langle\Psi_0|$. P_0 однозначно уничтожает $|\Psi_1\rangle$, но будучи применен к $|\Psi_0\rangle$, дает положительный результат с вероятностью $P = 1 - \|\langle\Psi_0|\Psi_1\rangle\|^2 > 0$. Для P_1ситуация обратная. В итоге результатом измерения может быть $|\Psi_0\rangle$, $|\Psi_1\rangle$ или двусмысленность. На стадии обмена по открытому каналу Алиса и Боб исключают двусмысленные результаты, и в результате около $(1 - \|\langle\Psi_0|\Psi_1\rangle\|^2)/2$ переданных битов будут коррелированы.

Позже был представлен протокол с шестью состояниями – расширение BB84. В данном протоколе у системы существует шесть состояний – к стандартным

четырем добавляется еще один базис ($|0_c\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$; $|1_c\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$). Соответственно у носителя информации появляется еще два поляризационных состояния – лево- и правоциркулярное.

3.2. Алгоритмы с использованием решеток

Два наиболее известных алгоритма с использованием решеток – GGH и NTRUEncrypt. Криптосистема GGH, названная по первым буквам фамилий изобретателей (Goldreich – Goldwasser - Halevi), была опубликована в 1997г. Алгоритм основан на проблеме поиска ближайшего вектора, которая в свою очередь опирается на сложность редукции решетки. Если известен базис, в нем легко сгенерировать вектор, близкий к определенной точке решетки – например, отклониться от точки на небольшой вектор смещения. Однако если известен только результирующий вектор, без базиса исходную точку не найти.

В 1999г. алгоритм был проверен вьетнамским криптоаналитиком Фонгом Нгуеном.

Некоторые прикладные применения задач из теории решеток изложены в [5, 6, 16, 19].

3.2.1. GGH

Как и любой алгоритм ассиметричного шифрования, GGH имеет открытый и закрытый ключи. С помощью открытого ключа любой может зашифровать сообщение, но прочитать такой шифртекст сможет только тот, кто знает закрытый ключ.

Дана решетка L. Секретный ключ – базис B в этой решетке и унимодулярная матрица U. Открытым ключом будет базис $B' = UB$. Пусть нам дано искажение e и требуется зашифровать сообщение $X = (x_1, x_2, \dots, x_n)$. Вычислим матрицу $v = XB'$. Шифртекстом будет матрица $C = v + e$.

Для расшифровки сначала вычислим $C' = CB^{-1}$:

$$C' = CB^{-1} = (XB' + e)B^{-1} = XUBB^{-1} + eB^{-1} = XU + eB^{-1}.$$

Слагаемое eB^{-1} обнуляем из соображений приближения, а слагаемое XU умножаем на матрицу U^{-1}. Получаем исходное сообщение.

Пример: Пусть нам нужно передать сообщение $X = (5; -6)$ решетка $L \subset \mathbb{R}^2$, вектор ошибки $e = (1; -1)$, а базис B задан следующей матрицей:

$$B = \begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}, B^{-1} = \begin{pmatrix} \frac{1}{5} & 0 \\ 0 & \frac{1}{4} \end{pmatrix}.$$

Возьмем матрицу U:

$$U = \begin{pmatrix} 7 & 4 \\ 5 & 3 \end{pmatrix}, U^{-1} = \begin{pmatrix} 3 & -4 \\ -5 & 7 \end{pmatrix}.$$

Получаем:

$$B' = UB = \begin{pmatrix} 35 & 16 \\ 25 & 12 \end{pmatrix},$$

$$C = XB' + e = (26; 7).$$

Для расшифровки умножим полученный вектор C на матрицу B^{-1}:

$$CB^{-1} = (5.2; 1.75).$$

После округления получившегося вектора умножаем его на U^{-1}:

$$X = (5; 2)U^{-1} = (5; -6).$$

Получили исходное сообщение X.

В 1999г. Фонг Нгуен показал, что система GGH не лишена недостатков. На конференции CRYPTO он продемонстрировал, что по зашифрованному тексту можно узнать некоторую уточняющую информацию о тексте исходном, а

проблему подбора ближайшего вектора при вскрытии шифра можно значительно упростить.

3.2.2. NTRUEncrypt

Алгоритм NTRUEncrypt, изначально называвшийся NTRU, был представлен в 1996г. на конференциях CRYPTO, RSA Conference и Eurocrypt. В этом же году математики Джеффри Хоффстейн, Джилл Пайфер, Джозеф Сильверман и основатель NTRU Cryptosystems Inc. Даниель Лайман запатентовали свое изобретение.

NTRU оперирует в кольце R усеченных многочленов степени, не превосходящей $N-1$. Для уменьшения коэффициентов многочленов используется деление по модулю на взаимно простые числа p и q.

Для передачи сообщения от Алисы к Бобу необходимы открытый и закрытый ключи. Для этого из кольца R Боб выбирает два полинома f и g, такие что:

1. f имеет df коэффициентов, равных единице, и $df-1$ коэффициентов, равных -1. Все остальные коэффициенты равны нулю.
2. g имеет dg коэффициентов, равных единице, и dg коэффициентов, равных -1. Все остальные равны нулю.

Поскольку $g(1)=0$, у полинома g не будет обратного элемента.

Далее, Бобу нужно вычислить еще два полинома f_p и f_q, такие что $f * f_p \equiv 1\,(mod\ p)$ и $f * f_q \equiv 1(mod\ q)$. Если какой-то из этих двух полиномов не существует, Бобу следует выбрать другой полином f и повторить операции с ним.

Пара (f, f_p) является секретным ключом, а элемент $h = (pf_q * g)(mod\ q)$ – открытый ключ.

Для того чтобы зашифровать сообщение, Алисе нужно представить сообщение в виде полинома X с коэффициентами по модулю p. Коэффициенты следует

выбирать из диапазона $\left(-\frac{p}{2};\frac{p}{2}\right]$. Далее необходимо выбрать полином r, такой что dr его коэффициентов равны единице и dr коэффициентов равны -1, все остальные равны нулю. Шифрованное сообщение получается из исходного по формуле:

$$Y = (r * h + X)(mod\ q).$$

Получив Y, Боб может расшифровать его с помощью своего секретного ключа. Для этого ему сначала нужно получить промежуточный полином $t_1 = (f * X)(mod\ q) = \left(f * \left(r * pf_q * g + X\right)\right)(mod\ q) = (pr * g + f * X)(mod\ q)$. Далее, Боб вычисляет второй промежуточный полином $t_2 = t_1\ (mod\ p)$. Поскольку $(pr * g)(mod\ p) = 0$, $t_2 = (f * X)(mod\ p)$. Далее, из t_2 Боб получает исходное сообщение:

$$X = \left(f_p * b\right)(mod\ p).$$

NTRUEncrypt имеет ряд преимуществ перед современными алгоритмами асимметричного шифрования. Во-первых, согласно[14], NTRUEncrypt на 4 порядка быстрее RSA и на 3 порядка – ECC. Во-вторых, при сопоставимой длине ключа криптостойкость NTRUEncrypt немного выше аналогов. Из недостатков следует отметить использование только рекомендуемых параметров для обеспечения наибольшей криптостойкости.

По мнению автора, алгоритм NTRUEncrypt является перспективной темой для дальнейших исследований. В диссертационной работе автором предполагается модернизация алгоритма с применением ортогональных базисных функций[12].

Подробнее описание алгоритмов, а также базовые знания в теории решеток и в криптографии на ее основе содержатся в [7, 8, 15, 17, 20]. Разбор алгоритмов NTRUEncrypt и NTRUSign – ЭЦП на основе алгоритма NTRU – содержится в [18].

3.3. Иные алгоритмы

Применение базисов в криптографии за пределами теории решеток и квантовых протоколов передачи данных началось совсем недавно, но, несмотря на это, уже существуют многообещающие алгоритмы, доступные для шифрования самой разной информации.

Когда речь заходит об аудиосигналах, на сцену снова выходят вейвлеты. В 2010г. А.И. Савватин и С.А. Новоселов из Ярославского государственного университета им. П.Г. Демидова предложили метод построения цифровой системы защищенной передачи речевой информации[9]. Вейвлеты в данной системе применяются для того же, для чего и в кодировании – с их помощью производится разложение сигнала на последовательность коэффициентов аппроксимации и последовательность детализирующих коэффициентов. Зашифрованный сигнал выглядит как аддитивная сумма коэффициентов сигнала и коэффициентов белого шума. Если вейвлет-функции, раскладывающие зашифрованный сигнал, ортогональны аппроксимирующей функции, то коэффициенты белого шума возможно отделить от коэффициентов сигнала. Требуемые вейвлет-фильтры можно построить с помощью вейвлетов Хаара, Добеши, но это не обеспечит должную секретность, т.к. указанные вейвлеты общеизвестны. Требуются уникальные ортогональные вейвлет-фильтры, которые и будут ключом в данном алгоритме. Кроме того, возможно построение вейвлет-функций, характеристики которых будут зависеть от ключевой последовательности.

3.3.1. Система защищенной передачи речевой информации

Авторами предложен алгоритм построения согласованных вейвлет-фильров, которые в сочетании с ортогональным ДВП позволяют разделять зашифрованный поток на помехи и исходный сигнал. Для релизации

ортогонального ДВП необходимо, чтобы амплитудно-частотная характеристика фильтра $H(\omega)$ удовлетворяла следующим условиям:

1. Положительность: $|H(\omega)| \geq 0$
2. Ортогональность: $|H(\omega)|^2 + |H(\pi - \omega)|^2 = 2$
3. Наличие нулевых моментов ЧХ: $H(\pi) = 0$

Пусть имеется некоторая функция $s(n)$. Нужно построить для нее набор ортогональных вейвлет-фильтров таким образом, чтобы при разложении $f(n) = IFFT\{S(\omega) * (1 + e^{-j\omega})\}$, где $S(\omega)$ – образ Фурье функции $s(n)$, на коэффициенты все детализирующие коэффициенты были равны нулю. Как оказалось, у данной задачи есть решение.

Пусть $S_A(\omega)$ и $S_D(\omega)$ – образы Фурье соответственно аппроксимирующих и детализирующих коэффициентов вейвлет-преобразования. Пусть также $H(\omega)$ и $G(\omega)$ – частотные характеристики низкочастотного и высокочастотного фильтров разложения. Тогда процедура вейвлет-преобразования $s(n)$ в частотной области будет выглядеть следующим образом:

$$\begin{cases} H(\omega)F(\omega) + H(\omega + \pi)F(\omega + \pi) = S_A(\omega) \\ G(\omega)F(\omega) + G(\omega + \pi)F(\omega + \pi) = S_D(\omega) \end{cases}.$$

Т.к. требуется наличие как минимум одного нулевого момента ЧХ фильтра, определим $F(\omega) = S(\omega) * (1 + e^{-j\omega})$. Теперь можно утверждать, что между фильтрами H и G установлено следующее соотношение:

$$G(\omega) = e^{-j\omega} * H^*(\omega + \pi).$$

В итоге выполняется одно из условий данных фильтров. Пусть $\overline{H(\omega)}$ и $\overline{G(\omega)}$ – частотные характеристики соответствующих фильтров восстановления. Тогда

$$G(\omega + \pi) * \overline{G(\omega)} + H(\omega + \pi) * \overline{H(\omega)} = 0.$$

Поскольку детализирующие коэффициенты предполагаются равными нулю, представим $S_D(\omega) = 0$ и решим исходную систему:

$$H(\omega) = \frac{A(\omega) * F(\omega)}{|F(\omega)|^2 + |F(\omega + \pi)|^2}.$$

Учитывая накладываемое на фильтры условие ортогональности и тот факт, что $S_A(\omega) = S_A(\omega + \pi)$, получаем

$$|S_A(\omega)|^2 = 2(|F(\omega)|^2 + |F(\omega + \pi)|^2).$$

Пусть $S_A(\omega)$ является действительной функцией. Тогда

$$S_A(\omega) = \sqrt{2(|F(\omega)|^2 + |F(\omega + \pi)|^2)}.$$

И окончательный результат:

$$H(\omega) = \frac{\sqrt{2} * F^*(\omega)}{\sqrt{F(\omega)^2 + |F(\omega + \pi)|^2}}.$$

Синтез СВФ для известных заранее вейвлетов Добеши, которые использовались в качестве исходного сигнала, показал, что данный метод ортогонализирует исходный сигнал, создавая новый вейвлет-базис. Как и ожидалось, были получены соответствующие фильтры Добеши.

В результате были найдены вейвлет-фильтры, с помощью которых можно восстанавливать сигнал только по аппроксимирующим коэффициентам. Импульсная характеристика фильтров формируется с учетом характеристик обрабатываемого сигнала (в данном случае это ключевая последовательность). Таким образом, информация о сигнале закладывается в сам фильтр.

3.3.2. Всплесковые базисы

Год спустя Д.С. Лукомский и С.Ф. Лукомский предложили универсальный алгоритм шифрования информации, в основе которого лежит идея разложения конечномерного вектора по ортонормированной системе[11]. Сама ортонормированная система определяется набором комплексных чисел $(\mu_k)_{k=0}^{N}$, и выполнены следующие условия:

- $\mu_0 = 1$
- $\forall k > 0: |\mu_k| = 1$

Последовательность $(\mu_k)_{k=0}^{N}$ можно использовать в качестве ключа.

Пусть дана $(G, \dot{+})$ - нуль-мерная локально компактная Абелева группа с цепочкой подгрупп

$$\ldots \subset G_n \subset \cdots \subset G_1 \subset G_0 \subset G_{-1} \subset \cdots \subset G_{-n} \subset \cdots; (G_n/G_{n+1})^{\#} = p,$$

Где p – простое. $g_n \in G_n/G_{n+1}$- базисная последовательность. Пусть также $r_n \in G_n^{\perp}/G_{n+1}^{\perp}$ - функция Радемахера, где $G_n^{\perp}$ - аннулятор подгруппы G_n. Возьмем исходное сообщение $X = (x_0, x_1, \ldots, x_{p-1})$.

Алгоритм шифрования следующий:

1. Выбираем последовательность $(\mu_k)_{k=0}^{p-1}$, отвечающую двум вышеупомянутым условиям.
2. Строим функцию $\varphi(x)$:

$$\varphi(x) = \frac{1}{p} G_{-1}(x) \sum_{j=0}^{p-1} \mu_j (r_{-1}, x)^j.$$

3. Образуем матрицу $M = (\varphi(\lambda_{g-1} \dot{-} \nu_{g-1}))_{\lambda,\nu}$.
4. Получаем шифртекст Y по формуле $Y = MX^T$.

При шифровании сообщение разбивается на блоки длиной p, каждый такой блок шифруется отдельно и независимо от других.

Т.к. $|\mu_j| = 1$, μ_j можно представить в виде $\mu_j = e^{\frac{2\pi i}{N+1} k_j}$, где $k_j = \overline{0, N}$. Вещественный вектор $K = (k_0, \ldots, k_N)$ тоже можно использовать в качестве ключа. Такой формат ключа больше подходит для компьютерной интерпретации алгоритма.

4. Заключение

Хотя исследования ведутся не один десяток лет, в наши дни работающих прототипов квантовых компьютеров очень немного, и самые современные ограничены 512 кубитами. Тем не менее, разработки криптоалгоритмов, устойчивых к атакам с помощью квантовых компьютеров, ведутся уже давно, поскольку актуальность данной темы очевидна в обозримом будущем.

Разработка защищенного канала передачи данных также является актуальной темой современной криптографии, ведь ни один самый стойкий алгоритм шифрования не дает стопроцентной защиты от атаки вида «человек посередине». Разработка алгоритмов передачи данных по квантовому каналу в теории может решить данную проблему.

Уже имеющиеся разработки доказывают, что базисы могут найти свое применение в криптографии, в том числе квантовой и постквантовой. Количество исследований растет с каждым годом, но данная тема еще далека от своего исчерпания и, по мнению автора, с годами будет только набирать актуальность.

5. Список литературы

1. *Молотков С.Н.* Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // ЖЭТФ – 2004 - т. 79, №11 - с. 691 – 704
2. *Голубчиков Д.М., Румянцев К.Е.* Квантовая криптография: принципы, протоколы, системы – Таганрог: ТТИ ЮФУ, 2008 – 37с.
3. *Молотков С.Н.* О стойкости волоконной квантовой криптографии при произвольных потерях в канале связи: запрет измерений с определенным исходом // ЖЭТФ – 2014 – т. 100, №6 – с. 457 – 464
4. *Скобелев В.Г.* Анализ атак на квантовый протокол передачи ключа // Прикладная дискретная математика – 2008 - №2 – с. 62 - 66
5. *M. Ruckert* Lattice-Based Blind Signatures // Advances in cryptology – ASIACRYPT 2010, pp 413 - 430
6. *D. Cash* Bonsai Trees, or How to Delegate a Lattice Basis / David Cash, Dennis Hofheinz, Eike Kiltz, Chris Peikert // Advances in cryptology – EUROCRYPT 2010, pp 523 - 552
7. *O. Regev* Lattice-Based Cryptography // Advances in cryptology – CRYPTO 2006, pp 131 - 141
8. *Шокуров А.В., Кузюрин Н.Н., Фомин С.А.* Решетки, алгоритмы и современная криптография – 2011, 130с.
9. *Савватин А.И., Новоселов С.А.* Метод построения цифровой системы защищенной передачи речевой информации // Вычислительные сети: теория и практика. 2010. Т.17, №2
10. *Левина А.Б.* Сплайн-вэйвлеты и их некоторые применения: диссертация кандидата физико-математических наук – СПб, 2009 – 214с.
11. *Лукомский Д.С., Лукомский С.Ф.* Всплесковые базисы и криптография // Сб. науч. тр. Механика. Математика, Саратов: Изд-во Сарат. ун-та, 2011. С. 55-58

12. *Леонтьев В.Л.* Ортогональные финитные функции и численные методы – Ульяновск: Изд-во УлГУ, 2003 - 177с.
13. *Демьянович Ю.К., Левина А.Б.* О вэйвлетных разложениях линейных пространств над произвольным полем и о некоторых приложениях // Математическое моделирование – т.20, №11 – 2008 – с.104 - 108
14. *J. Hermans, F. Vercauteren, B. Preneel* Speed Records for NTRU, Topics in Cryptology - CT-RSA 2010, pp73-88 (2010)
15. *D. Micciancio, O. Regev* Lattice-based Cryptography // Post-Quantum Cryptography – 2009 – pp 147 – 191
16. *C. Peikert* Lattice Cryptography for the Internet // Post-Quantum Cryptography – 2014 – pp 197 – 219
17. *D. Micciancio* Lattice Based Cryptography // Encyclopedia of Cryptography and Security – 2005 – pp 347 – 349
18. *J. Hoffstein, N. Howgrave-Graham, J. Pipher, W. White* Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign // The LLL Algorithm – 2010 – pp 349 – 390
19. *S. Wang, Y. Zhu, D. Ma, R. Feng* Lattice-based key exchange on small integer solution problem // Science China Information Sciences – vol. 57, issue 11 – 2014 – pp 1 – 12
20. *J. Hoffstein* Lattices and cryptography // An Introduction to Mathematical Cryptography – 2008 – pp 1 – 87
21. *Молотков С.Н.* О стойкости практической квантовой криптографии: протокол распределения ключей BB84 // ЖЭТФ – 2—8 – т.134, вып. 1 (7) – с. 39 – 64
22. *M. Naggy, N. Naggy* Quantum based secure communications with no prior key distribution // Soft computing, 2014