Автор:

Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный

исследовательский университет

им. академика С.П. Королева»

г. Самара, Самарская область

КРИПТОГРАФИЯ НА ОСНОВЕ КОДОВ ИСПРАВЛЕНИЯ ОШИБОК

Аннотация: *в данной статье рассмотрены распространенные алгоритмы шифрования Niederreiter и McEliece. В последнее время считается наиболее перспективным кандидатом на роль постквантовой криптосистемы именно McEliece.*

Ключевые слова: *криптография, корректирующие коды, исправление ошибок.*

Введение

При хранения информации под влиянием помех, а также в процессе передачи, могут возникать ошибки. Что бы обнаружить и исправить ошибки, используются специальные корректирующие коды (коды обнаружения и исправления ошибок).

Для проверки или исправлении ошибок во время процессов записи или передачи к информативным данным добавляют контрольное число (особым образом структурированную избыточную информацию). Количество ошибок, поддающихся исправлению, полностью зависит от выбранного применяемого кода.

Коды обнаружения могут только проверить существование ошибки, но не исправить, в отличии от кодов исправления. Но обнаружить их могут и используемые коды исправления, так как они принадлежат одним классам кодов.

$К_{об} > К_{исп}$, где $К_{об}$ – количество обнаруженных ошибок, а $К_{исп}$ – исправленных.

Существуют криптосистемы с открытыми ключами, на основании кодов исправления ошибок. Самыми распространенными являются алгоритмы шифрования Niederreiter и McEliece.

Криптосистема McEliece

Разработал Робертом Мак-Элисом данную криптосистему с открытыми ключами в 1978 году. В ней впервые использовалась рандомизация в процессе зашифровки. Основанием алгоритма является сложность процесса декодирования полных линейных кодов.

Получить открытый ключ можно путем перемножения производящей матрицы G на невырожденные случайные матрицы S и P. В качестве закрытого ключа выступает код исправления ошибок, количество которых равно t, а также применяется эффективный алгоритм декодирования. Как правило в алгоритме оперируют двоичные коды Гоппа. McElice, где используются коды Гоппа, до сих пор не поддается криптоанализу.

Недостатки криптосистемы McEliece

В наше время эта криптосистема не получила широкого применения в силу некоторых недостатков. Например, из-за размера открытого ключа, он слишком большой (при использовании кодов Гоппы открытый ключ будет 2^{19} бит), шифротекст длиннее в разы исходного сообщения, система сильнее подвержена ошибкам при передаче сообщения, и не может быть использована для аутентификации.

Алгоритм работы McEliece

Криптосистема использует 3 этапа:

1. Генерация ключа, выдающего открытый и закрытый ключ.

А. Выбирается двоичный (n,k) – линейный код C, который исправляет t ошибок. Для кода C вычисляется k x n производящая матрица G.

Б. Генерируются случайные n x n матрица перестановки P и невырожденная k x k матрица S.

В. Высчитывается k x n матрица G"=SGP.

Г. Закрытый ключ представляет собой набор (S,G,P), а открытый ключ пару (G",t).

2. Шифрование передаваемого сообщения.

А. Сообщение m представляется в виде последовательности бинарных символов длины k.

Б. Вычисляется вектор c"=mG".

В. Генерирование случайного вектора z длины n, содержащего в себе t единиц.

Г. Вычисляется зашифрованное сообщение c=c" + z.

3. Расшифровка принятого зашифрованного сообщения.

А. Вычисление обратных матриц P^{-1} и S^{-1}.

Б. Вычисление $c'=c P^{-1}$.

В. Используется алгоритм расшифровки для кода C (двоичные коды Гоппа легко декодируются с помощью алгоритма Петерсона), для получения m' из c'.

Г. Вычисление исходного сообщения $m=m'S^{-1}$.

Перспективы использования McEliece

Ведутся разработки учеными по созданию квантовых компьютеров. И рано или поздно они достигнут в этом успеха, и будут созданы квантовые компьютеры.

Нынешние системы шифрования построены на сложных математических задачах, которые требуют очень длительного перебора для нахождения решения. Это поиск дискретных логарифмов, криптография на основе эллиптических кривых, разложение целых чисел на простые множители. Простые компьютеры не могут справиться с ними за приемлемое время, однако это не будет проблемой для квантовых компьютеров.

Всей современной популярной криптографии с открытыми ключами придет конец, как только их работоспособность перейдет в полную силу. ECC, DH, RSA, DSA и другие криптоалгоритмы для обмена цифровых подписей и ключей утратят свою силу.

Из-за этого в последние годы ведутся стремительные исследования алгоритмов, которые на квантовых компьютерах будут устойчивы к взлому.

Такие алгоритмы уже существуют и хорошо изучены. Их можно считать квантово-устойчивыми, так как не зависят от квантовых вычислений. В последнее время считается наиболее перспективным кандидатом на роль постквантовой криптосистемы именно McEliece.