Применение реберного локального дополнения в структурном анализе криптосистемы Мак-Элиса

Соколова Анастасия Александровна

Студентка

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: soko.anastasiia@gmail.com

В криптосистеме Мак-Элиса одному и тому же открытому ключу могут соответствовать несколько секретных ключей, следовательно, они могут быть разбиты на классы эквивалентности. Возможность подобрать эквивалентный ключ напрямую влияет на стойкость этого метода шифрования, так как ключ для расшифрования не уникален. Имеющиеся исследования в данной области рассматривают ограниченный набор кодов с тривиальной группой автоморфизмов и неприменимы в структурном анализе криптосистемы Мак-Элиса. Возникает проблема поиска альтернативы предложенным методам, применимой к циклическим кодам.

С помощью простых преобразований двоичный линейный код можно представить в виде двудольного графа. Вводимая в [1] операция ELC (edge local complemetation, реберное локальное дополнение) над ним позволяет рассматривать различные эквивалентные коды, а орбита двудольного графа под ELC является полным классом эквивалентности для кода, отвечающего данному графу. Этот способ не зависит от структуры кода. Данный метод представления и обработки графов позволяет по-новому представить классы эквивалентности двоичных кодов и классифицировать все ELC-орбиты кодов различной длины. Двоичный линейный [n, k] код $\boldsymbol{C}$ соответствует двудольному графу на n вершинах с матрицей смежности определенного вида. Применение любой последовательности ELC-операций к графу G, соответствующему коду $\boldsymbol{C}$ преобразует его в граф, код которого эквивалентен $\boldsymbol{C}$.

В данной работе на языке C были предложены и реализованы алгоритм для нахождения и перечисления классов эквивалентности циклических кодов с помощью графов и операции ELC, а также алгоритм для сравнения двух кодов на эквивалентность, один из которых является циклическим. В рамках этих реализаций получена полная классификация циклических кодов длины 19.

Первый алгоритм строит по длине порождающего полинома циклического кода все возможные графы, проводит ELC-

преобразования, находит изоморфные графы и подсчитывает количество классов эквивалентности (число орбит). В качестве входного набора данных генерируются все возможные порождающие многочлены указанной пользователем длины. Операция ELC над циклическими кодами не выводит за рамки циклических кодов, значит, можно сказать, что все орбиты будут состоять только из них, и, находя все орбиты, мы находим все циклические коды, эквивалентные данному.

Во втором алгоритме сравнение происходит следующим образом: для данного циклического графа строится орбита, после чего в ней ищется второй граф, приведенный к требуемому виду. В случае обнаружения можно утверждать, что графы эквивалентны, иначе — обратное.

При сужении класса исследуемых кодов до циклических значительно возрастает эффективность алгоритма, что априорно не ясно из структуры метода. Был улучшен достигнутый ранее результат скорости и качества вычислений. В [1] на суперкомпьютере были подсчитаны классы эквивалентности для графов с числом вершин не более 12 (примерное время — 1 месяц). На пользовательском компьютере удалось реализовать вычисления для 10 вершин (ок. 1200 сек.). В текущей работе только на пользовательском компьютере удалось работать с графами с 17 вершинами (код длины 19, вычисление количества классов эквивалентности заняло ок. 8 суток). Программа сравнения двух кодов, один из которых циклический, на эквивалентность, на персональном компьютере вычисляет эквивалентность или ее отсутствие для кодов длины 19.

Литература

1. Danielsen L. E., Parker M. G. Edge local complementation and equivalence of binary linear codes. // Designs, Codes and Cryptography 49, 2008.
2. Чижов И. В. Пространство ключей криптосистемы Мак-Элиса–Сидельникова. // Диссертация, кафедра информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова, защищена в 2010 г.
3. Östergård P. R. J. Classifying subspaces of Hamming spaces. // Designs, Codes and Cryptography 27, 2002.
4. Sendrier N. The Support Splitting Algorithm. [Research Report] // RR-3637, INRIA. 1999.
5. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки М.: Связь, 1979.