КРИПТОГРАФИЧЕСКАЯ СИСТЕМА ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОЛЯРНЫХ КОДОВ

С.Б. Саломатин, М.А. Алисеенко

Полярные коды достигают граничных параметров и используются в системе сотовой связи 5G [1]. Представляет интерес рассмотреть особенности полярных кодов для защиты канала передачи данных [2].

Один из возможных методов защите может быть основан на методике сокрытия порождающей матрицы полярных кодов, структура которой зависит от канала. Предполагается, что злоумышленник имеет неограниченный доступ к каналу передачи и может определить генераторную матрицу, используя параметры канала, длину и размер предполагаемого полярного кода.

Алгоритм защиты генераторной матрицы.

1. Определяются параметры Бхаттачатрия битовых каналов, и перестановка.

2 Индексы выбираются случайным образом из индексов хороших битовых каналов. Этот шаг эквивалентен случайному выбору битовых каналов из хороших битовых каналов.

3. Секретная матрица определяется как подматрица, строки которой выбираются на основе индексов замороженного набора секретов.

4. Замороженный вектор имеет криптографическую защиту.

Эффективность. Существует большого семейства эквивалентных полярных кодов, которое приводит к повышению уровня защиты от атак с исчерпывающим поиском. Матрицы полярных кодов имеют особую структуру, которая позволяет уменьшить размер ключа. Несистематичность полярных кодов, позволяет декодировать особые формы преднамеренных векторов ошибок, что обеспечивает более высокий уровень защиты от выбранных атак с открытым текстом при меньшей длине ключа.

Литература

1. Rosenqvist T., Sloof J. Implementation and evaluation of Polar Codes in 5G. Karlstad University, 2019.

2. Mahdavifar H., Vardy A. Achieving the secrecy capacity of wiretap channels using polar Codes // IEEE Trans. Inf. Theory. 2011. Vol. 57, iss. 10. P. 6428–6443.