ЗАЩИТА ИНФОРМАЦИИ ПРИ НОРМЕННОЙ ОБРАБОТКЕ ИНФОРМАЦИИ

Н.З. ХОАНГ

Проблема защиты информации приобрела актуальность в связи с быстрым развитием инфокоммуникационных систем, при проектировании которых необходимо передавать данные с максимальной скоростью и минимальными потерями при воздействии помех. Для этого широко используется помехоустойчивое кодирование для защиты информации от искажений, возникающих в канале связи. Борьба с многократными искажениями данных является весьма трудоемкой задачей из-за проблемы «селектора».

На рубеже 20–21 века белорусской школой кодирования была предложена теория норм синдромов, с помощью которой можно снизить на порядок влияния проблемы «селектора». Однако при увеличении кратности корректируемых ошибок, а также длины кодов сложность реализации декодеров остается вновь ощутимой.

В данной работе рассматривается подход к сжатию норм путем отображения корректируемых ошибок в ошибки большего веса, но со значениями синдромов, содержащими нулевую ту или иную компоненту, что позволяет уменьшить множество норм. В работе исследовали три случаи, когда равны нулю, соответственно первая, вторая и третья компонента синдрома. Сравнение этих случаев показывает следующее.

Наиболее эффективным методом является придание значения первой компоненты синдрома. При этом достигается шестикратное сжатие множества селектируемых норм. Для кода БЧХ n=31, t=3 исходная норма N_3 принимает все значения от единицы до 30, а после сдвига до $S_1=\alpha^0$ и суммирования с вектором $(\alpha^0, \alpha^0, \alpha^0)$ первого столбца проверочной матрицы $H=(\alpha^t, \alpha^{3t}, \alpha^{5t})^T$, N_3^{**} принимает только 5 значений; для кода n=31, t=4 с фиксированной нормой

N_5^{**}, суммарное число норм N_4^{**} также равно 5 (при синдроме $S=[s_1, s_2, s_3]^T=(\alpha^i, \alpha^j, \alpha^z)^T$ $N_3=3z-5j$, а при синдроме $S=[O, s_2^{**}, s_3^{**}]^T=[\alpha^i, \alpha^j, \alpha^{z**}]^T$ $N_3^{**}=3z^{**}-5j^{**}$). Замечено уменьшение количества используемых норм: для кода БЧХ с $n=31$, $t=3$, при использовании без сжатия требуется три нормы (N_1, N_2, N_3) в качестве идентификационных параметров, а после преобразования, когда $S_1=0$, только две нормы (N_1, N_3^{**}), для кода $n=31$, $t=4$ — шесть норм (N_1, N_2, N_3, N_4, N_5, N_6), после преобразования, когда $S_1=0$, требуется только три нормы (N_1, N_4^{**}, N_5^{**}), что позволяет в десятки раз уменьшить сложность реализации декодера при больших длинах кодов.