УДК 004.056.55

Увеличение расстояния единственности при компрессии и шифровании текста с элементами кодирования.

А.А. Бабаев, И.И. Кротов

[1]Московский физико-технический институт (государственный университет)

В работе рассмотрен метод увеличения расстояния единственности с целью усложнения дешифрования злоумышленником информации, который реализуется следующим образом:

1) Сжатие открытого текста M_0 битовой длины N, в результате чего получается текст M_1 длины $N_1 = \alpha N$ и не изменяется его энтропия, где α — коэффициент сжатия [1]. Если в результате компрессии удалось достичь того, что все символы выпадают равновероятно, то энтропия будет равна $H(M_1) \approx \alpha N$ [2].

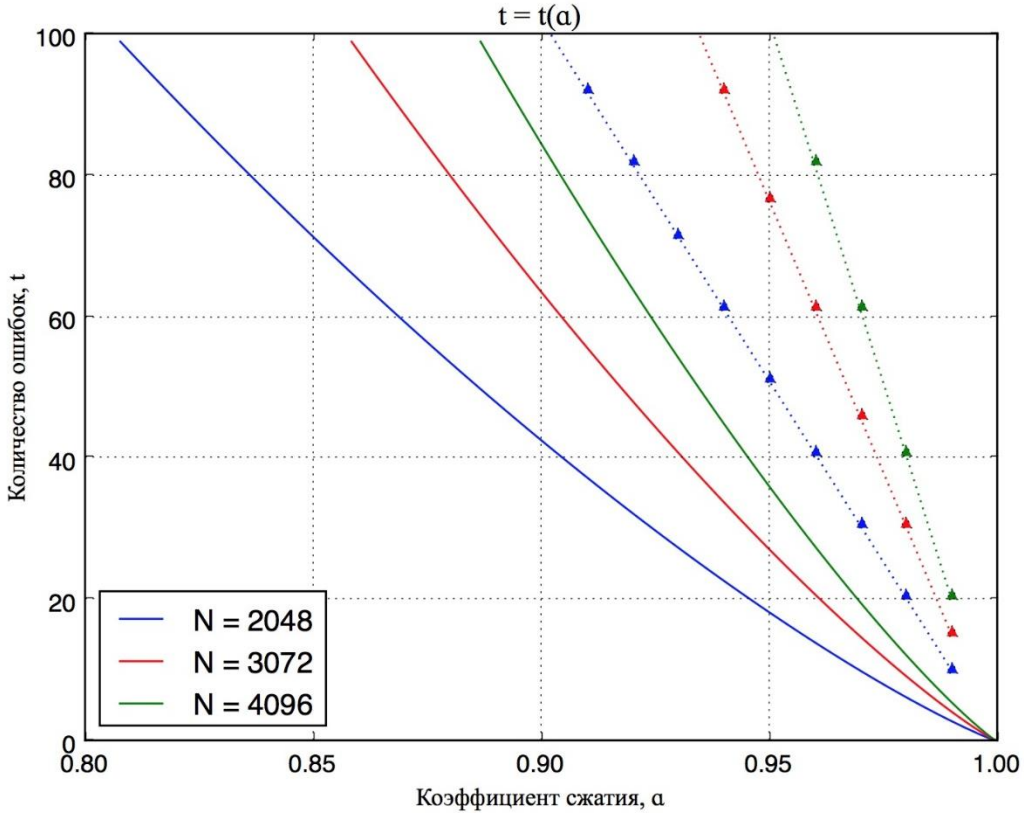
2) Шифрование текста с помощью системы Мак-Элиса [3], тем самым возвращая исходную длину текста $N_2 = \beta N_1 = \alpha\beta N = N$. Энтропия в таком случае имеет оценку Хэмминга сверху [4]:

$$H(M_2) \le N\left(1 - \frac{\log_2 \sum_{k=0}^{t} C_N^k}{N}\right),$$

где t — число вносимых ошибок. В результате мы получим открытый текст длины исходного сообщения с уменьшенной энтропией при условии, что

$$\left(1 - \frac{\log_2 \sum_{k=0}^{t} C_N^k}{N}\right) \le \alpha.$$

Далее приведены графики зависимости возможного числа вносимых ошибок t от максимального коэффициента сжатия текста α при различных длинах открытого текста, чтобы было выполнено неравенство. Также на графике изображены соответствующие границы Синглтона.



Идея метода заключается в том, что после проведения вышеописанных процедур уменьшится энтропия открытого текста, в результате чего увеличится расстояние единственности. Согласно [5]

$$n_u = \frac{H(K)}{\left(1 - \frac{H(M)}{N \log_2 L}\right) \log_2 L},$$

где n_u — расстояние единственности, $H(K)$ — энтропия ключа, $H(M)$ — энтропия открытого текста, $L = 2$ — число символов в алфавите, N — число бит в слове. Поскольку энтропия ключа, длина текста и число символов в алфавите — константы, то уменьшив энтропию, что было показано в данной работе, увеличивается расстояние единственности.

В итоге был получен алгоритм, позволяющий при сжатии сообщения и последующего шифрования с помощью системы Мак-Элиса отправлять зашифрованные сообщения длиной исходного сообщения.

Литература

1) *Сэломон Д.* Сжатие данных, изображений и звука //М.: Техносфера. – 2004. – Т. 368.
2) *Габидулин Э. М., Пилипчук Н. И.* Лекции по теории информации. — М.: МФТИ, 2007. — С. 16. — 214 с. — ISBN 5-7417-0197-3.
3) *McEliece R. J.* A public-key cryptosystem based on algebraic //Coding Thv. – 1978. – Т. 4244. – С. 114-116.
4) *Сагалович Ю. Л.* Введение в алгебраические коды: учебное пособие. — 3-е изд., перераб. и доп. — М.: ИППИ РАН, 2014. — 310 с. — ISBN 978-5-901158-24-1
5) *Габидулин Э. М., Кшевецкий А. С., Колыбельников А. И.* Расстояние единственности // Защита информации: учебное пособие — М.: МФТИ, 2011. — 225 с. — ISBN 978-5-7417-0377-9