★★★　＜知的財産翻訳検定＞答案用紙　★★★

==========

科　　目：電気・電子工学

氏　　名：坂本礼子

==========

What is claimed is:

1. An encryption communication apparatus comprising:

an encryption recording means including:

an error-correction encoding means that performs error-correction encoding by adding redundancy to inputted data;

an interleaving means that sorts the data outputted from the error-correction encoding means by a predetermined bit number according to a previously specified rule, and outputs the sorted data; and

an encoding means that encodes the outputted data from the interleaving means so as to keep content of the outputted data from the interleaving means secret; and

an encryption reproducing means including:

a decoding means that decodes inputted data that is data outputted from the encryption recording means reproduced from any recording medium;

a de-interleaving means that sorts, so as to restore an order of the data sorted by the interleaving means, the data outputted from the decoding means by a predetermined bit number according to a previously specified rule, and outputs the data sorted by the de-interleaving means; and

an error-correction decoding means that corrects an error in the data outputted from the de-interleaving means, based on the redundancy added by the error-correction encoding means.

2. The encryption communication apparatus according to Claim 1, wherein

each means included in the encryption recording means and each means included in the encryption reproducing means are given information for operation from respective key information generating means.

In the encryption reproducing means, the data outputted from the encryption recording means is decoded by the decoding means 5. Consecutive errors in the data outputted from the decoding means 5 that have been caused by errors in the data generated in the given recording medium are converted to random pseudo-errors by the de-interleaving means 6. FIGs. 3A, 3B, and 3C illustrate the above operation. Assuming that the encoding means 3 and decoding means 5 are block ciphers, when errors are generated in the data inputted to the decoding means 5 in the process of

reproduction from the recording medium, consecutive errors are generated in the blocks having errors during inputted as shown by a block Bi in a reference numeral 13 in FIG 3A. Also assuming that the de-interleaving means 6 is such that, in a memory structure by a matrix as shown by a reference numeral 14 in FIG. 3B, sequentially writing in a column direction of a row is performed when writing and sequentially reading in a row direction of a column is performed when reading, the block Bi having the error is written to an i-th row in the memory of the de-interleaving means 6, and the data in the block Bi having the error appears dispersed in an i-th bit of each column when reading (Pj, i 16 in Pj15 in FIG. 3C). As described above, in blocks having consecutive errors in the data outputted from the decoding means 5 are dispersed by the de-interleaving means 6, and the errors in the data outputted from the de-interleaving means 6 appear almost randomly.