METHOD AND APPARATUS FOR ENCRYPTION HAVING A FEEDBACK REGISTER WITH SELECTABLE TAPS

Abstract of the Invention

A method and apparatus for generating a pseudo-random bit sequence is provided. A first input bit (260) is determined as a function of bits stored in a shift register (252) in accordance with a first feedback algorithm. In addition, a second input bit (262) is determined as a function of bits stored in the shift register (252) in accordance with a second feedback algorithm. Subsequently, a particular input bit (268) to be provided to the shift register (252) is deterministically selected from the group consisting of the first input bit (260) and the second input bit (262) such that a non-linear pseudo random sequence may be produced by the shift register (252). In addition, a communication unit which utilizes the pseudo-random bit sequence in encrypting a signal to be transmitted and decrypting a received signal is described.

FIG. 2 accompanies this abstract.