

PSEUDORANDOM FUNCTION AND THE USE THEREOF FOR ENCRYPTION

ABSTRACT

5 A software-efficient pseudorandom function maps an index and an
encryption key to a pseudorandom bit string useful for constructing a
stream cipher. The method begins by preprocessing the encryption key
into a table of pseudorandom values. The index and a set of values from
10 the table is then used to generate a set of initial values for the
registers. At least some of the register values are modified in part by
taking a current value of a register and replacing the current value with
a function of the current value and a value retrieved from the table, the
latter value being determined by the values in one or more other
15 registers. After modifying the register values in this fashion, the
values are masked using other values from the table and the results then
concatenated into the pseudorandom bit string. The modification step is
repeated and a new masked function of the register values is then
concatenated into the pseudorandom bit string. The modification and
concatenation steps are repeated to continue growing the pseudorandom bit
20 string until the string reaches some desired length.

This Sheet Has Been Replaced