ABSTRACT E-101/1953/2013

GENERATION OF RANDOMIZED MESSAGES FOR CRYPTOGRAPHIC HASH FUNCTIONS

Method(s) and system(s) (105) for generation of randomized messages for cryptographic hash functions are described herein. The method includes obtaining a random value based on a randomization criterion to randomize a message. Further, a last data block of the message is populated with a randomization parameter to obtain a randomized message. The randomization parameter populated in the last block is computed using the random value.

<<To be published with Fig. 1>>

I/We claim:

1. A randomized message generation system (105) comprising::

   processor(s) (125);

   a primary randomization module (145) coupled to the processors (125), the primary randomization module (145) obtains a random value based on a randomization criterion to randomize a message; and

   a secondary randomization module (150) coupled to the processors (125), the secondary randomization module (150) populates a last data block of the message with a randomization parameter to obtain a randomized message for use in a cryptographic hash function, wherein the randomization parameter is computed using the random value.

2. The randomized message generation system (105) as claimed in claim 1, wherein the secondary randomization module (150) further determines:

   space occupied by padding bits in the last data block;

   available space in the last data block based on the space occupied by the padding bits and message bits in the last data block to compute the randomization parameter.

3. The randomized message generation system (105) as claimed in claim 1, wherein the primary randomization module (145) is further:

   determines a block length of a compression function, wherein the compression function is a component of the cryptographic hash function used for hashing the randomized message;

   divides the message into a predetermined number of data blocks based on the block length of the compression function; and

   concatenates the random value to itself a predetermined number of times, based on the block length of the compression function.

4. The randomized message generation system (105) as claimed in claim 3, wherein the secondary randomization module (150) randomizes each of the predetermined number of data blocks using the concatenated random value, wherein the concatenated random value is mixed with a data block using a mixing function.

5. The randomized message generation system (105) as claimed in claim 1, wherein the secondary randomization module (150) is further: